



VERIFICATION OF TRANSLATION

I, Kiyoshi Tanaka, of c/o SAKAI International Patent Office, 2-6, Kasumigaseki 3-chome, Chiyoda-ku, Tokyo 100-0013 Japan, hereby declare that I am a translator of the document attached, and attached document is a true and correct translation made by me to the best of my knowledge and belief.

Japanese Patent Application No.2001-094342, filed on March 28, 2001

Signature of Translator: Kiyoshi Tanaka  
Kiyoshi Tanaka

Date : December 28, 2004



(TRANSLATION)

PATENT OFFICE  
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this Office.

DATE OF APPLICATION : March 28, 2001

APPLICATION NUMBER : Japanese Patent Application  
No. 2001-094342

APPLICANT(S) : Ricoh Co., Ltd.

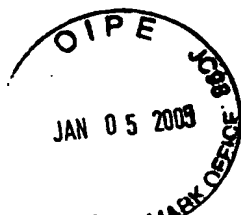
Issued :

Commissioner,  
Patent Office

(Official Seal)

Certificate No.

[TYPE OF DOCUMENT] APPLICATION FOR PATENT  
[REFERENCE NO.] 0007340  
[FILING DATE] March 28, 2001  
[ADDRESS TO] COMMISSIONER, PATENT OFFICE  
[INTL' CLASSIFICATION] G06F 17/60  
[TITLE OF INVENTION] Image formation system, software  
acquisition method, and computer-readable recording medium  
having recorded therein program for making computer execute the  
method  
[NUMBER OF CLAIMS] 27  
[INVENTOR]  
[ADDRESS] c/o Ricoh Co., Ltd.  
3-6, Nakamagome 1-chome, Ohta-ku  
Tokyo, Japan  
[NAME] Hiroyuki Matsushima  
[APPLICANT FOR PATENT]  
[CODE NO.] 000006747  
[NAME] Ricoh Co., Ltd.  
[AGENT]  
[CODE NO.] 100089118  
[PATENT ATTORNEY]  
[NAME] Hiroaki SAKAI  
[PRIORITY CLAIM BASED ON PRIOR APPLICATION]  
[APPLICATION NO.] Japanese Patent Application  
No. 2000-264710  
[FILING DATE] August 31, 2000  
[INDICATION OF FEE]  
[NUMBER] 036711  
[AMOUNT OF FEE] 21000  
[LIST OF ATTACHED DOCUMENTS]  
[ITEM] SPECIFICATION 1  
[ITEM] DRAWINGS 1  
[ITEM] ABSTRACT 1  
[GENERAL POWER OF ATTORNEY NUMBER] 9808514



[Type of Document] ~~Japanese~~ Specification

[Title of the Invention] Image formation system, software acquisition method, and computer-readable recording medium having recorded therein program for making computer execute the method

5 [Scope of Claims for Patent]

[Claim 1] An image formation system comprising:

an image formation apparatus connected to a network, said image formation apparatus having one or more hardware resources of a display section, an operation panel section, a printing section, and an image  
10 pickup section, wherein said image formation apparatus is capable of providing one or more services of a printer, a copier, or a facsimile; and

a server connected to the network, said server providing a software component to said image formation apparatus via said network, wherein said image formation apparatus includes,

15 a selection unit that selects a desired software component from a list of software components accumulated in said server and displayed on said display section;

an acquisition unit that acquires the software component selected by said selection unit and authentication information from said  
20 server; and

a control unit that controls processing operation of the software component acquired by said acquisition unit based on the authentication information acquired by said acquisition unit.

[Claim 2] The image formation system according to claim 1,  
25 wherein said control unit restricts a range of resources available for the

software components, of resources provided in said image formation apparatus, based on the authentication information.

[Claim 3] The image formation system according to claim 2, wherein

5 when authentication based on the authentication information has failed, said control unit controls so that said display section and operation panel section of the resources become available for the software components, and controls so that all the resources become available for the software components when the authentication based on the  
10 authentication information has succeeded.

[Claim 4] The image formation system according to claim 3, wherein

the authentication information includes information related to rights for using the respective resources by the software components,  
15 and

said control unit decides whether the software components can use the resources based on the information related to the using rights.

[Claim 5] The image formation system according to any one of claims 1 to 4, wherein said image formation apparatus further comprises  
20 a transmission unit that transmits configuration information for said image formation apparatus to said server when succeeding in the authentication based on the authentication information, and

said server dynamically organizes software components executable on said image formation apparatus based on the configuration  
25 information received from said image formation apparatus, and sends the

organized software components back to said image formation apparatus.

[Claim 6] The image formation system according to claim 5,  
wherein

said transmission unit transmits identification information for  
5 identifying said image formation apparatus to said server, and  
said server identifies one or more of configuration information and  
a contract form of said image formation apparatus based on the  
identification information received from said image formation apparatus,  
dynamically organizes software components executable on said image  
10 formation apparatus based on the identified configuration information  
and/or contract form, and sends the organized software components back  
to said image formation apparatus.

[Claim 7] The image formation system according to any one of  
claims 1 to 6, wherein said server is a WWW server functioning on the  
15 Internet, and

said image formation apparatus further provides a browser with  
which pages described in HTML are browsed.

[Claim 8] The image formation system according to claim 7,  
wherein the software component acquired by said acquisition unit  
20 operates as a plug-in for said browser.

[Claim 9] The image formation system according to claim 7,  
wherein said image formation apparatus further establishes a virtual  
machine that can execute CPU-independent intermediate code, and the  
virtual machine executes the software components accumulated in said  
25 server in the form of the intermediate code.

[Claim 10] The image formation system according to any one of claims 1 to 9, wherein, one vendor manages said server, and an another vendor can register a software component to said server by paying a particular registration fee to the vendor that manages the server.

5 [Claim 11] The image formation system according to any one of claims 1 to 10, wherein the vendor is charged for an advertisement fee of a software component each time said image formation apparatus acquires the software component from said server.

[Claim 12] The image formation system according to any one of  
10 claims 1 to 11, wherein a server of the third-party vendor can be registered with said image formation apparatus as a server allowed to be authenticated when the third-party pays a particular registration fee.

[Claim 13] The image formation system according to any one of claims 1 to 12, wherein one or more of a charge for using said image  
15 formation apparatus and the registration fee paid by the third-party vendor is changed according to a range of resources available for said image formation apparatus.

[Claim 14] A software acquisition method in an image formation system which connects an image formation apparatus and a server to a  
20 network, said image formation apparatus having hardware one or more of resources of a display section, an operation panel section, a printing section, and an image pickup section and for providing one or more of services of a printer, a copier, or a facsimile, and said server providing a software component to said image formation apparatus, wherein said  
25 image formation apparatus performing the steps of:

selecting a desired software component from a list of software components accumulated in said server and displayed on said display section;

acquiring the selected software component and authentication  
5 information from said server; and

controlling a processing operation of the acquired software component based on the acquired authentication information.

[Claim 15] The software acquisition method according to claim 14, wherein the controlling step restricts a range of resources available  
10 for the software component, of resources provided in said image formation apparatus, based on the authentication information.

[Claim 16] The software acquisition method according to claim 15, wherein,

when authentication based on the authentication information has  
15 failed, the controlling step controls so that said display section and operation panel section of the resources become available for the software components, and controls so that all the resources become available for the software components when authentication based on the authentication information has succeeded.

20 [Claim 17] The software acquisition method according to claim 16, wherein

the authentication information includes information related to rights for using the respective resources by the software components, and

25 the controlling step decides whether the software components can



use the resources based on the information related to the using rights.

[Claim 18] The software acquisition method according any one of claims 14 to 17, further comprising a step of transmitting configuration information for said image formation apparatus to said server when said  
5 image formation apparatus has succeeded in authentication based on the authentication information, wherein

said server dynamically organizes software components executable on said image formation apparatus based on the configuration information received from said image formation apparatus, and sends the  
10 organized software components back to said image formation apparatus.

[Claim 19] The software acquisition method according to claim 18, wherein

in the transmitting step, identification information for identifying said image formation apparatus is transmitted to said server, and  
15 said server identifies one or more of configuration information and a contract form of said image formation apparatus based on the identification information received from said image formation apparatus, dynamically organizes software components executable on said image formation apparatus based on the identified configuration information  
20 and/or contract form, and sends the organized software components back to said image formation apparatus.

[Claim 20] The software acquisition method according to any one of claims 14 to 17, wherein said server is a WWW server functioning on the Internet, and  
25 said image formation apparatus has a browser with which pages

described in HTML are browsed.

[Claim 21] The software acquisition method according to claim 20, wherein the software component acquired in the acquiring step operates as a plug-in for said browser.

5 [Claim 22] The software acquisition method according to claim 20, wherein said image formation apparatus has a virtual machine that can execute CPU-independent intermediate code, and the virtual machine executes the software components accumulated in said server in the form of the intermediate code.

10 [Claim 23] The software acquisition method according to any one of claims 14 to 22, wherein, one vendor manages said server, and another vendor can register a software component to said server by paying a particular registration fee to the vendor that manages the server.

[Claim 24] The software acquisition method according to any 15 one of claims 14 to 23, wherein the vendor is charged for an advertisement fee of a software component each time said image formation apparatus acquires the software component from said server.

[Claim 25] The software acquisition method according to any one of claims 14 to 24, wherein a server of the third-party vendor can be 20 registered with said image formation apparatus as a server allowed to be authenticated when the third-party pays a particular registration fee.

[Claim 26] The software acquisition method according to any one of claims 14 to 25, wherein one or more of a charge for using said image formation apparatus and the registration fee paid by the third-party 25 vendor is changed according to a range of resources available for said

image formation apparatus.

[Claim 27] A computer readable recording medium having stored therein a program for causing a computer to realize the method according to any one of claims 14 to 26.

5

[Detailed Description of the Invention]

[0001]

[Field of the Invention]

The present invention relates to an image formation system  
10 including an image formation apparatus having one or more hardware  
resources of a display section, an operation panel section, a printing  
section, and an image pickup section, wherein the image formation  
apparatus is capable of providing one or more services of a printer, a  
copier, or a facsimile; and a server that provides a software component to  
15 the image formation apparatus to the image forming apparatus. The  
image forming apparatus and the server are connected to each other via  
a network. The present invention relates to a software acquiring method  
for the system and a computer-readable recording medium having  
recorded therein a program for making computer execute the method. In  
20 particular, the present invention relates to an image forming system,  
software acquiring method, and a recording medium that enables  
legitimately and efficiently acquiring and executing software components  
pertinent to the operation of the image formation apparatus after the  
image formation apparatus has been activated.

25

[0002]

[Prior Art]

Conventionally, a printer, a copier, and a facsimile have been generally provided as discrete devices. Recently, there is known an image formation apparatus in which functions of the above-mentioned  
5 devices are accommodated into one cabinet (hereafter called "multifunction machine").

[0003]

This multifunction machine has a display section, printing section, and an image pickup section within one cabinet, and also has software  
10 corresponding to a printer, copier, and a facsimile device. Switching the software allows the machine to operate as the printer, copier, or the facsimile device

[0004]

If such a multifunction machine is available, the cost and space  
15 can be in total reduced, because, there is no need to separately provide the printer, the copier, and the facsimile device.

[0005]

[Problems to be Solved by the Invention]

However, such multifunction machines are generally delivered to  
20 a client after pre-installing desired softwares that perform predetermined functions. Therefore, the important matter is how to adequately update the existing functions or add new functions after the multifunction machine has been delivered.

[0006]

25 For example, when a technology of downloading software from a

server through a network and executing it on a multifunction machine is employed, it is necessary to avoid downloading of malicious software from an unauthorized server and to refuse an access request to software from an unauthorized terminal that impersonates an authorized multifunction machine.

[0007]

Even if a copier is authorized, it is not appropriate to permit the copier to execute any functions other than functions previously contracted. Further, even if the functions are previously contracted, it is not worth downloading the functions (software) if they are useless from the viewpoint of a hardware configuration of the copier. Based on these facts, it is important to legitimately and efficiently acquire and execute software adequate for a multifunction machine after the multifunction machine is activated.

[0008]

It is an object of this invention to provide an image formation system capable of legitimately and efficiently acquiring and executing software adequate for an image formation apparatus after the image formation apparatus is activated, and to provide a software acquisition method and a computer-readable recording medium where a computer program for making a computer execute the method is recorded.

[0009]

[Means to Solve the Problems]

To solve the above-mentioned problems and achieve the above-mentioned objects, the image formation system according to claim

1 of this invention comprises an image formation system comprising: an  
image formation apparatus connected to a network, said image formation  
apparatus having one or more hardware resources of a display section,  
an operation panel section, a printing section, and an image pickup  
5 section, wherein said image formation apparatus is capable of providing  
one or more services of a printer, a copier, or a facsimile; and a server  
connected to the network, said server providing a software component to  
said image formation apparatus via said network, wherein said image  
formation apparatus includes, a selection unit that selects a desired  
10 software component from a list of software components accumulated in  
said server and displayed on said display section; an acquisition unit that  
acquires the software component selected by said selection unit and  
authentication information from said server; and a control unit that  
controls processing operation of the software component acquired by said  
15 acquisition unit based on the authentication information acquired by said  
acquisition unit.

[0010]

According to the invention of claim 1, the image formation  
apparatus selects a desired software component from a list of software  
20 components accumulated in the server, acquires the software component  
selected and authentication information from the server; and controls  
processing operation of the software component, so that the processing  
operation of the software component can be changed based on the result  
of authentication.

25

[0011]

The image formation system according to claim 2 of this invention is characterized in that in the invention of claim 1, said control unit restricts a range of resources available for the software components, of resources provided in said image formation apparatus, based on the authentication information.

[0012]

According to the invention of claim 2, said control unit restricts a range of resources available for the software components, of resources provided in said image formation apparatus, based on the authentication information, so that the operation of the software component acquired from a server of which authentication has failed can be restricted.

[0013]

The image formation system according to claim 3 of this invention is characterized in that in the invention of claim 2, when authentication based on the authentication information has failed, said control unit controls so that said display section and operation panel section of the resources become available for the software components, and controls so that all the resources become available for the software components when the authentication based on the authentication information has succeeded.

[0014]

According to the invention of claim 3, when authentication based on the authentication information has failed, said control unit controls so that said display section and operation panel section of the resources become available for the software components, and controls so that all

the resources become available for the software components when the authentication based on the authentication information has succeeded. Accordingly, when the authentication has failed, it is controlled such that only the minimum resources are available.

5 [0015]

The image formation system according to claim 4 of this invention is characterized in that in the invention of claim 3, the authentication information includes information related to rights for using the respective resources by the software components, and said control unit decides  
10 whether the software components can use the resources based on the information related to the using rights.

[0016]

According to the invention of claim 4, the authentication information includes information related to rights for using the respective  
15 resources by the software components, and said control unit decides whether the software components can use the resources based on the information related to the using rights, so that a decision whether the software can use the resources can be made speedily and efficiently.

[0017]

20 The image formation system according to 5 is characterized in that in the invention of any one of claims 1 to 4, said image formation apparatus further comprises a transmission unit that transmits configuration information for said image formation apparatus to said server when succeeding in the authentication based on the authentication  
25 information, and said server dynamically organizes software components



executable on said image formation apparatus based on the configuration information received from said image formation apparatus, and sends the organized software components back to said image formation apparatus.

[0018]

5           According to the invention of claim 5, said image formation apparatus transmits configuration information for said image formation apparatus to said server when succeeding in the authentication based on the authentication information, and said server dynamically organizes software components executable on said image formation apparatus  
10   based on the configuration information received from said image formation apparatus, and sends the organized software components back to said image formation apparatus. Accordingly, when succeeding in the authentication, an optimal software component that is adapted to the software configuration and hardware configuration of the image forming  
15   apparatus can be acquired.

[0019]

          The image formation system according to 6 is characterized in that in the invention of claim 5, said transmission unit transmits identification information for identifying said image formation apparatus to  
20   said server, and said server identifies one or more of configuration information and a contract form of said image formation apparatus based on the identification information received from said image formation apparatus, dynamically organizes software components executable on said image formation apparatus based on the identified configuration  
25   information and/or contract form, and sends the organized software

components back to said image formation apparatus.

[0020]

According to the invention of claim 6, said transmission unit transmits identification information for identifying said image formation apparatus to said server, and said server identifies one or more of configuration information of the image forming apparatus and a contract form of said image formation apparatus based on the identification information received from said image formation apparatus, dynamically organizes software components executable on said image formation apparatus based on the identified configuration information and/or contract form, and sends the organized software components back to said image formation apparatus. Accordingly, an optimal software component that is adapted to the software configuration, hardware configuration of the image forming apparatus or the contract form can be acquired.

[0021]

The image formation system according to 6 is characterized in that in the invention of any one of claims 1 to 6, said server is a WWW server functioning on the Internet, and said image formation apparatus further provides a browser with which pages described in HTML are browsed.

[0022]

According to the invention of claim 7, said server is a WWW server functioning on the Internet, and said image formation apparatus further provides a browser with which pages described in HTML are

browsed, so that the image forming apparatus and the server can perform transmission according to the HTTP protocol.

[0023]

The image formation system according to 8 is characterized in  
5 that in the invention of claim 7, the software component acquired by said acquisition unit operates as a plug-in for said browser.

[0024]

According to the invention of claim 8, the software component  
acquired operates as a plug-in for said browser, so that the software  
10 component can be easily and speedily executed.

[0025]

The image formation system according to 9 is characterized in  
that in the invention of claim 7, said image formation apparatus further  
establishes a virtual machine that can execute CPU-independent  
15 intermediate code, and the virtual machine executes the software  
components accumulated in said server in the form of the intermediate  
code.

[0026]

According to the invention of claim 9, said image formation  
20 apparatus further establishes a virtual machine that can execute  
CPU-independent intermediate code, and the virtual machine executes  
the software components accumulated in said server in the form of the  
intermediate code. Accordingly, the same software component can be  
executed in different types of image forming apparatus.

25 [0027]

The image formation system according to 10 is characterized in that in the invention of any one of claims 1 to 9, one vendor manages said server, and an another vendor can register a software component to said server by paying a particular registration fee to the vendor that  
5 manages the server.

[0028]

According to the invention of claim 10, one vendor manages said server, and an another vendor can register a software component to said server by paying a particular registration fee to the vendor that manages  
10 the server, so that it is possible for a third-party vender to register the software component without causing disadvantages to the primary vender.

[0029]

The image formation system according to 11 is characterized in  
15 that in the invention of any one of claims 1 to 10, the vendor is charged for an advertisement fee of a software component each time said image formation apparatus acquires the software component from said server.

[0030]

According to the invention of claim 11, the vendor is charged for  
20 an advertisement fee of a software component each time said image formation apparatus acquires the software component from said server, so that the vendor who has developed the software component and the primary vendor can be treated impartially.

[0031]

25 The image formation system according to 12 is characterized in

that in the invention of any one of claims 1 to 11, a server of the third-party vendor can be registered with said image formation apparatus as a server allowed to be authenticated when the third-party pays a particular registration fee.

5 [0032]

According to the invention of claim 12, a server of the third-party vendor can be registered with said image formation apparatus as a server allowed to be authenticated when the third-party pays a particular registration fee, so that appropriate burden can be imposed to the

10 third-party vendor.

[0033]

The image formation system according to 13 is characterized in that in the invention of any one of claims 1 to 12, one or more of a charge for using said image formation apparatus and the registration fee paid by

15 the third-party vendor is changed according to a range of resources available for said image formation apparatus.

[0034]

According to the invention of claim 13, one or more of a charge for using said image formation apparatus and the registration fee paid by

20 the third-party vendor is changed according to a range of resources available for said image formation apparatus, so that appropriate charge for use and/or registration fee can be charged according to the range of resources available.

[0035]

25 The software acquisition method according to 14 is a software

acquisition method in an image formation system which connects an image formation apparatus and a server to a network, said image formation apparatus having hardware one or more of resources of a display section, an operation panel section, a printing section, and an image pickup section and for providing one or more of services of a printer, a copier, or a facsimile, and said server providing a software component to said image formation apparatus, wherein said image formation apparatus performing the steps of: selecting a desired software component from a list of software components accumulated in said server and displayed on said display section; acquiring the selected software component and authentication information from said server; and controlling a processing operation of the acquired software component based on the acquired authentication information.

[0036]

According to the software acquisition method of the invention of claim 14, said image formation apparatus selects a desired software component from a list of software components accumulated in said server and displayed on said display section; acquires the selected software component and authentication information from said server; and controls a processing operation of the acquired software component based on the acquired authentication information. Accordingly, the processing operation of the software component can be changed based on the result of the authentication.

[0037]

The software acquisition method according to 15 is characterized

in that in the invention of claim 14, the controlling step restricts a range of resources available for the software component, of resources provided in said image formation apparatus, based on the authentication information.

[0038]

5           According to the invention of claim 15, a range of resources available for the software component, of resources provided in said image formation apparatus, is controlled based on the authentication information, so that the operation of the software component acquired from the server that has failed authentication can be restricted.

10           [0039]

          The software acquisition method according to 16 is characterized in that in the invention of claim 15, when authentication based on the authentication information has failed, the controlling step controls so that said display section and operation panel section of the resources become  
15   available for the software components, and controls so that all the resources become available for the software components when authentication based on the authentication information has succeeded.

[0040]

          According to the invention of claim 16, when authentication based  
20   on the authentication information has failed, the controlling step controls so that said display section and operation panel section of the resources become available for the software components, and controls so that all the resources become available for the software components when authentication based on the authentication information has succeeded.  
25   Accordingly, it is possible to control such that when the authentication has

failed, only the minimum resources can be used.

[0041]

The software acquisition method according to 17 is characterized in that in the invention of claim 16, the authentication information includes  
5 information related to rights for using the respective resources by the software components, and the controlling step decides whether the software components can use the resources based on the information related to the using rights.

[0042]

10 According to the invention of claim 17, the authentication information includes information related to rights for using the respective resources by the software components, and the controlling step decides whether the software components can use the resources based on the information related to the using rights. Accordingly, the decision as to  
15 whether software components can use the resources can be made speedily and efficiently.

[0043]

The software acquisition method according to 18 is characterized in that in the invention of any one of claims 14 to 17, the method  
20 comprises a step of transmitting configuration information for said image formation apparatus to said server when said image formation apparatus has succeeded in authentication based on the authentication information, wherein said server dynamically organizes software components executable on said image formation apparatus based on the configuration  
25 information received from said image formation apparatus, and sends the



organized software components back to said image formation apparatus.

[0044]

According to the invention of claim 18, said image formation apparatus transmits configuration information for said image formation apparatus to said server when said image formation apparatus has  
5 succeeded in authentication based on the authentication information, and said server dynamically organizes software components executable on said image formation apparatus based on the configuration information received from said image formation apparatus, and sends the organized  
10 software components back to said image formation apparatus.

Accordingly, an optimal software component that is adapted to the software configuration and hardware configuration of the image forming apparatus can be acquired when the authentication has succeeded.

[0045]

15 The software acquisition method according to 19 is characterized in that in the invention of claim 18, in the transmitting step, identification information for identifying said image formation apparatus is transmitted to said server, and said server identifies one or more of configuration information and a contract form of said image formation apparatus based  
20 on the identification information received from said image formation apparatus, dynamically organizes software components executable on said image formation apparatus based on the identified configuration information and/or contract form, and sends the organized software components back to said image formation apparatus.

25

[0046]

According to the invention of claim 19, the identification information for identifying said image formation apparatus is transmitted to said server, and said server identifies one or more of configuration information and a contract form of said image formation apparatus based on the identification information received from said image formation apparatus, dynamically organizes software components executable on said image formation apparatus based on the identified configuration information and/or contract form, and sends the organized software components back to said image formation apparatus. Accordingly, an optimal software component that is adapted to the software configuration and hardware configuration of the image forming apparatus, or contract form can be acquired when the authentication has succeeded.

[0047]

The software acquisition method according to 20 is characterized in that in the invention of any one of claims 14 to 19, said server is a WWW server functioning on the Internet, and said image formation apparatus has a browser with which pages described in HTML are browsed.

[0048]

According to the invention of claim 20, said server is a WWW server functioning on the Internet, and said image formation apparatus has a browser with which pages described in HTML are browsed, so that the image forming apparatus and the server can perform communication based on the HTTP protocol..

[0049]

The software acquisition method according to 20 is characterized in that in the invention of claim 20, the software component acquired in the acquiring step operates as a plug-in for said browser.

[0050]

5           According to the invention of claim 21, the software component acquired in the acquiring step operates as a plug-in for said browser, so that the software component can be easily and speedily executed.

[0051]

10           The software acquisition method according to 22 is characterized in that in the invention of claim 20, said image formation apparatus has a virtual machine that can execute CPU-independent intermediate code, and the virtual machine executes the software components accumulated in said server in the form of the intermediate code.

[0052]

15           According to the invention of claim 22, said image formation apparatus has a virtual machine that can execute CPU-independent intermediate code, such as Java Applet, and the virtual machine executes the software components accumulated in said server in the form of the intermediate code. Accordingly, the same software component can be  
20           executed in different types of image forming apparatus.

[0053]

            The software acquisition method according to 23 is characterized in that in the invention of any one of claims 14 to 22, one vendor manages said server, and an another vendor can register a software  
25           component to said server by paying a particular registration fee to the

vendor that manages the server.

[0054]

According to the invention of claim 22, one vendor manages said server, and another vendor can register a software component to said server by paying a particular registration fee to the vendor that manages the server, so that it is possible for a third-party vendor to register the software component without causing disadvantages to the primary vendor.

[0055]

The software acquisition method according to 24 is characterized in that in the invention of any one of claims 14 to 23, the vendor is charged for an advertisement fee of a software component each time said image formation apparatus acquires the software component from said server.

[0056]

According to the invention of claim 24, the vendor is charged for an advertisement fee of a software component each time said image formation apparatus acquires the software component from said server, so that the vendor who has developed the software component and the primary vendor can be treated impartially.

[0057]

The software acquisition method according to 25 is characterized in that in the invention of any one of claims 14 to 24, a server of the third-party vendor can be registered with said image formation apparatus as a server allowed to be authenticated when the third-party pays a

particular registration fee.

[0058]

According to the invention of claim 25, a server of the third-party vendor can be registered with said image formation apparatus as a server  
5 allowed to be authenticated when the third-party pays a particular registration fee, so that appropriate burden can be imposed to the third-party vendor.

[0059]

The software acquisition method according to 26 is characterized  
10 in that in the invention of any one of claims 14 to 25, one or more of a charge for using said image formation apparatus and the registration fee paid by the third-party vendor is changed according to a range of resources available for said image formation apparatus.

[0060]

15 According to the invention of claim 26, one or more of a charge for using said image formation apparatus and the registration fee paid by the third-party vendor is changed according to a range of resources available for said image formation apparatus, so that appropriate charge for use and/or registration fee can be charged according to the range of  
20 resources available.

[0061]

The computer readable recording medium according to 27 has stored therein a program for causing a computer to realize the method according to any one of claims 14 to 26 so that the medium can be read  
25 by a computer. Accordingly, any one of the operation according to any

one of claims 14 to 26 can be realized by the computer.

[0062]

[Embodiments of the Invention]

[0062]

5           Embodiments of the image formation system, the software acquisition method, and the computer-readable recording medium according to this invention will be explained in detail below with reference to the accompanying drawings.

[0063]

10           The system construction of the image formation system according to an embodiment of this invention will be explained first. Fig. 1 is a block diagram showing the system construction of the image formation system and the hardware configuration of the multifunction machine 10 according to this embodiment.

15           [0064]

As shown in Fig. 1, this image formation system has the multifunction machine 10 that makes a request for a software component and the server 20 that provides the software component in response to the request from the multifunction machine 10, which are connected to  
20 each other through a network 30.

[0065]

This multifunction machine 10 has the CPU 11, ROM 12, RAM 13, flash memory 14, FAX controller 15, scanner 16, plotter 17, large-capacity storage device 18, and the network I/F section 19.

25           [0066]

The CPU 11 is a central processing unit that loads software stored in the ROM 12 or the flash memory 14 into a main storage device (RAM 13) and executes the software. The ROM 12 is a read only memory, the RAM 13 is a volatile memory that is readable and writable, and the flash memory 14 is an erasable nonvolatile memory. Embedded software can also execute the program stored in the ROM 12 without being loaded into the RAM 13.

[0067]

The FAX controller 15 controls facsimile transmission and reception, and the scanner 16 is an image input section that optically scans an original. The plotter 17 is an image output device that prints image data on printing paper, and the large-capacity storage device 18 is a secondary storage medium such as a hard disk that stores various types of software. The network I/F section 19 is a processing section that functions as an interface with the network 30.

[0068]

Fig. 2 is a block diagram showing the software configuration of the multifunction machine 10 shown in Fig. 1. The multifunction machine 10 shown in the figure displays a list of software components accumulated in the server 20 on the display section. When a user selects a required software component, the multifunction machine 10 downloads the software component accumulated on the server 20 into the machine to extend its own function.

[0069]

At this time, the multifunction machine 10 performs authentication

based on the authentication information received by the server 20, and decides whether each of the resources provided in the machine is allowed to be used based on the result of the authentication. That is, the component downloaded from the server, whose authentication has  
5 succeeded, can use all the functions of the machine. But restrictions are put on the functions to be used by the component downloaded from the server whose authentication has failed. For example, using a printing function and scanning function is restricted in an MFP, so that the MFP can execute only graphics display on the display section.

10 [0070]

When the machine transmits its own identification information (ID) to the server 20 whose authentication has succeeded, the server 20 can retrieve the customer information and displays the software components matching the information, or can transmit the list to the multifunction  
15 machine 10. Further, when the configuration information of the software or hardware is transmitted to the server 20, the server 20 can display the executable software components or transmit the list of the components to the multifunction machine 10.

[0071]

20 More specifically, as shown in Fig. 2, the multifunction machine 10 has the Black & White Line Printer (B&W LP) 101, Color Line Printer (Color LP) 102, and some other resources such as hardware resources 103, and has the software group 110 that consists of the platform 120 and the application 130.

25 [0072]



The platform 120 consists of the general purpose OS 121 and System Resource Manager (SRM) 123 having the System Control Service (SCS) 122, and various types of control services 141 to 145. The general purpose OS 121 is a general purpose operating system such as UNIX, and executes parallel processing of the respective control services on the platform 120 and the respective software of the application 130, each of which is a discrete process.

[0073]

By using the UNIX as open source, reliability of the program can be ensured, the OS can support for networks, and source code becomes easily available. Further, there is no need to pay royalties of OS and TCP/IP, and outsourcing is facilitated.

[0074]

The SRM 123 together with the SCS 122 controls the system and manages the resources, arranges the resources according to requests from a higher layer that uses the hardware resources: engines of the scanning section and printer section, memory, HDD file, and host I/O (Centronic I/F, network I/F, IEEE1394 I/F, RS232C I/F, etc.), and controls its execution.

[0075]

More specifically, the SRM 123 determines whether the requested hardware resource is available (whether the resource is being used by another request), and sends a message that the requested hardware resource is available to the higher layer when it is available. By scheduling usage of the hardware resources for the requests from the

higher layer, the SRM 123 may directly execute the contents of the request (e.g., paper conveyance and image forming operation by the printer engine, allocation of memory, and file creation, etc.).

[0076]

5           The SCS 122 performs processing such as (1) management of applications, (2) controlling of the operation panel section, (3) display of a system screen such as a job list screen and a counter display screen), (4) LED display, (5) management of resources, and (6) controlling of applications to interrupt. More specifically, for (1) management of  
10 applications, the SCS 122 performs registration of applications and notification of the information to another applications. The SCS 122 notifies a registered application of system setting and an engine status according to the setting requested from the application. The SCS 122 queries the application having been registered for transition of power  
15 mode or for whether transition of the system status such as interrupt mode is allowed.

[0077]

For (2) controlling of the operation panel section, the SCS 122 performs exclusive control for the using right of the operation panel  
20 section of the application. The SCS 122 then exclusively notifies the application having the using right of the operation panel section of the key information from the operation panel section driver (OCS). With this key information, mask control is performed to temporarily stop notification according to the transition of the system status such as during switching  
25 applications.

[0078]

In (3) display of the system screen, the SCS 122 displays alarm screens for each engine status according to the contents requested from the application having the using right of the operation panel section.

5 One of these screens turns on or off the alarm display such as a user-restricted screen according to the state of the application. Other than the engine status, the SCS 122 provides controls for a job list screen for displaying reservation and situations of executing jobs, a counter screen for displaying a total counter group, and a screen indicating during  
10 notification of CSS. With regard to display of these system screens, release of the using right of the operation panel section is not requested to the application, but the screen is rendered as a system screen that covers the application screen.

[0079]

15 In (4) LED display, the SCS 122 controls a display of alarm LED and a system LED such as application keys. The application uses directly the display driver to control the LED specific to the application.

[0080]

In (5) management of resources, when the application (ECS)  
20 executes a job, the SCS 122 provides service for exclusive control of the engine resources (scanner, staple, etc.) that have to be excluded. In (6) controlling of applications to interrupt, the SCS 122 provides control and service so as to preferentially operate a particular application.

[0081]

25 The control service includes Engine Control Service (ECS) 141,

Memory Control Service (MCS) 142, Operation panel Control Service (OCS) 143, FAX Control Service (FCS) 144, and Network Control Service (NCS) 145.

[0082]

- 5           The ECS 141 controls engines for the black and white line printer (B&W LP) 101, color line printer (Color LP) 102, and some other hardware resources 103, or the like, and performs processing such as image read, printing operation, its status notification, and jam recovery.

[0083]

- 10           More specifically, the ECS 141 performs a series of copying/scanning/printing operation by successively issuing print requests to the SRM 123 according to specification of the job mode received from the application 130. The jobs as targets to be handled by the ECS 141 are assumed to specify SCANNER in the image input device,  
15   or to specify PLOTTER in the image output device.

[0084]

- For example, in the case of the copy operation, "SCANNER → PLOTTER" is specified, "SCANNER → MEMORY" is specified for file accumulation, and "SCANNER → FAX\_IN" is specified for facsimile  
20   transmission. In the case of printing an accumulated file or printing from a printer application 131, "MEMORY → PLOTTER" is specified, while in the case of facsimile reception, "FAX\_OUT → PLOTTER" is specified.

[0085]

- Although the definition of a job depends on applications, a  
25   processing operation for a set of image groups handled by a user is

defined here as one job. For example, in the case of Automatic Document Feeder (ADF) mode of copy, the operation of reading a set of originals placed on a document support is defined as one job, and in a pressure plate mode, a read operation until a final original is confirmed is defined as one job. Further, in the case of a copier application 132, an operation of copying a bundle of originals is one job, an operation of transmitting one document or an operation of receiving one document is one job in the case of a facsimile application 133, and an operation of printing one document is one job in the case of the printer application 131.

[0086]

The MCS 142 performs memory control. More specifically, the MCS 142 performs processing such as acquisition and release of the image memory, utilization of a hard disk drive (HDD), and compression or decompression of the image data.

[0087]

Functions required for managing necessary information as image data files accumulated in the hard disk drive include (1) a file access (creation/deletion/open/close) function (including exclusive processing), (2) management of various types of file attributes (management of image data as files by each physical page) such as management of file names/IDs (files/users)/ passwords management/ accumulated time management/ the number of pages/ data formats (compression system, etc.)/ access restriction/ creation of an application/ management of printing conditions, (3) connection/insertion/cut functions by the file or

page, (4) a file sort function (accumulated time order/ user ID order, etc.), (5) notification (for display/ retrieval) of all file information, (6) a recovery function (abandon of a file/page of a damaged file), and (7) an automatic deleting function of files, or the like.

5 [0088]

As a function to hold image data in memory such as RAM and get access to the memory, there are (1) a function of acquiring a file and information for page/band attributes from the application 130, and (2) functions of allocating and releasing a region of image data from the application 130, and read and write functions of image data.

[0089]

The OCS 143 is a module that controls the operation panel as an information transmission unit between an operator and control of the main body, and performs processing of notifying the control of the main body of a key operating event by the operator, providing library functions required when the respective applications construct GUI, managing the constructed GUI information for each application, and of reflecting the information on the display of the operation panel, or the like.

[0090]

20 This OCS 143 has (1) a function of providing library for GUI architecture, (2) a function of managing hardware resources of the operation panel section, (3) VRAM drawing/LCD display functions (display of hardware, switching of displayed applications, switching of displayed languages, dark colored display on window, display of message/icon blink, and display of linked messages), (4) a hardware

25

key-entry detection function, (5) a touch panel key-entry detection function, (6) an LED output function, and (7) a beeper output function, and the like.

[0091]

5           The FCS 144 provides an API for facsimile transmission and reception using PSTN/ISDN network from each application layer of the system controller, registration/citation of various facsimile data managed by BKM (backup SRAM), facsimile reading, facsimile reception/ printing, or merged transmission and reception.

10           [0092]

More specifically, this FCS 144 has functions such as (1) a transmission function of transmitting a document requested for transmission from the application layer, to a facsimile receiver using the PSTN/ISDN network, (2) a reception function of forwarding and printing a  
15 facsimile reception screen received from the PSTN/ISDN network or various types of reports to each application layer, (3) a telephone directory citation/registration function of citing and registering facsimile management items such as a telephone directory or group information stored in a facsimile board, (4) a facsimile log notification function of  
20 notifying any application that requires history information for transaction results stored in BKM mounted on a facsimile board, of such history information, and (5) an event notification function of notifying an application registered in the FCS of a changed event when the status of the facsimile board is changed.

25           [0093]

The NCS 145 is a group of modules for providing commonly available services to any application requiring network I/O, assigns data received by each protocol from the network to each of the applications, and acts as a medium when the data is transmitted from the application to the network. More specifically, the NCS 145 has server daemons such as ftpd, httpd, lpd, snmpd, telnetd, or smtpd, and client functions having the same protocol.

[0094]

The application 130 has Page Description Language (PDL) and a printer application 131 as an application for a printer having PCL and PostScript (PS). This application 130 also has a copier application 132 as an application for a copier, a facsimile application 133 as an application for a facsimile, and a scanner application 134 as an application for a scanner. The application 130 further has a WWW browser 135 for browsing WWW (World Wide Web) pages as a distributed system on the Internet, a download application 136 that downloads a software component and so on from the server 20, and an authentication processing application 137 that performs authentication processing based on authentication information accepted from the server 20. The download application 136 and authentication processing application 137 will be explained in detail later.

[0095]

As explained above, the multifunction machine 10 encloses a common part between the application 130 and the control services as a platform 120, and places the control services 141 to 145 and the



applications 131 to 137 on this platform 120. Therefore, each of these control services 141 to 145 and applications 131 to 137 can be handled as a software component.

[0096]

5           The configuration of the server 20 shown in Fig. 1 will be explained below. Fig. 3 is a functional block diagram showing the configuration of the server 20 shown in Fig. 1. The server 20 is a WWW server that can browse pages using the WWW browser of the multifunction machine 10, and comprises the interface section 21,  
10 encryption processing section 22, authentication information transmission section 23, software component storage section 24, customization processing section 25, and the control section 26.

[0097]

15           The interface section 21 is a data input/output section that is connected to a LAN (Internet) using TCP/IP protocol and performs data transaction using HyperText Transfer Protocol (HTTP).

[0098]

20           The encryption processing section 22 encrypts authentication information consisting of a hash value of a software component using a secret key or a public key held inside the device. The authentication information transmission section 23 is a processing section that transmits authentication information in response to the request of the multifunction machine 10 when the multifunction machine 10 authenticates whether the server 20 has been registered.

25           [0099]

The software component storage section 24 is a software database that accumulates software components developed by the machine development vendor or third vendors. The customization processing section 25 is a processing section that retrieves a software component adequate for the model or the configuration of the multifunction machine 10 from the software component storage section 24 when receiving configuration information for the machine such as the software configuration or hardware configuration of the multifunction machine 10. The control section 26 controls the overall server 20, and outputs a request accepted from the multifunction machine 10 to a desired processing section according to the contents of the request.

[0100]

Downloading of a software component using the download application 136 of the multifunction machine 10 shown in Fig. 2 will be explained below in (1) a case of its performance with a plug-in, and (2) a case of its performance with Java Applet.

[0101]

(1) Performance of downloading with the plug-in

Fig. 4 is a flowchart showing the processing sequence when downloading is executed with the plug-in. Fig. 5A shows URLs of software components owned by the server, and Fig. 5B shows an example of HTML description.

[0102]

As shown in Fig. 5A, the software component placed in the server 20 has an extension of "gw", and the authentication information has an

extension of "aut". This figure also shows a URL of an HTML file including a link to a list of components, URL of a software component 1, URL of authentication information for the software component 1, URL of a software component 2, and a URL of authentication information for the software component 2.

[0103]

As shown in Fig. 4, the multifunction machine 10 displays the link on the browser (step S401), and when the user selects the link displayed on the browser and the reference destination of this link is the URL with the extension gw (step S402), the browser starts the plug-in for downloading the software.

[0104]

This plug-in converts first the extension of the target URL as reference destination to aut (step S403), and issues a request to the server (step S404). When receiving the request (step S405), the server transmits the authentication information to the multifunction machine 10 (step S406). Accordingly, this multifunction machine 10 acquires the authentication information (step S407).

[0105]

Subsequently, when the user accesses the target URL through the multifunction machine 10 (step S408), the server transmits a software component in response to this access (steps S409 to S410), and the multifunction machine 10 downloads the software component (step S411).

[0106]

The multifunction machine 10 then performs authentication

processing explained later (step S412), and executes the downloaded software component by the plug-in (step S413).

[0107]

Although "comp\_list.html" can be expressed as shown in Fig. 5B,  
5 HTML including the software component can also be described by using an EMBED tag and an object tag other than the tags shown here.

[0108]

(2) Performance of downloading with the Java Applet

When the reference destination of the link of a software  
10 component is an HTML file including Java Applet, the multifunction machine 10 can also download the software component described as this Java Applet and execute the component. However, in this case, the multifunction machine 10 is required to provide a Java Virtual Machine (JVM).

15 [0109]

Fig. 6 is a flow chart showing the processing sequence when the software component is downloaded using Java. Fig. 7A shows an example of the HTML file as a target to be linked, and Fig. 7B shows the software configuration of the multifunction machine 10 in the above case.

20 [0110]

As shown in Fig. 6, the multifunction machine 10 displays the link on the browser (step S601), and when the user selects the reference destination as shown in Fig. 7A on the browser to access the reference destination (steps S602 to S604), the multifunction machine 10  
25 downloads an applet (SoftwareComponentLoader.class) for downloading

a software component from the server 20 (steps S605 to S606).

[0111]

When this applet is executed on the JVM (step S607), the applet downloads the component indicated by the "software" parameter and the authentication information indicated by the "authentication" parameter (steps S608 to S611), performs authentication using the authentication information (step S612), and executes the software component on the JVM (step S613).

[0112]

10       The software configuration of the multifunction machine 10 in this case is as shown in Fig. 7B. A group of standard Java classes equipped by using the OCS and NCS and a group of control classes, that lap the respective ECS, MCS, SCS, and FCS, operate on the JVM. The downloaded component executes the processing using these class  
15   libraries.

[0113]

The authentication processing executed by the authentication processing application 137 shown in Fig. 2 will be specifically explained below in (1) a case of its performance with a common encryption key, (2)  
20   a case of its performance with a public key, and (3) a case of its performance with a certificate. The authentication information is assumed here to include a magic number of "RICOH", a hash value (Message Digest) of a software component, and using rights of resources. For example, the using rights of the resources are as follows:

25       permission.scanner=true

permission.plotter=false  
permission.storage=false  
permission.fax=false  
permission.panel=true  
5 permission.network=true  
[0114]

(1) Performance of authentication processing with the common encryption key

Fig. 8 is a flowchart showing the processing sequence of the  
10 multifunction machine 10 when authentication is performed using a common encryption key. Fig. 9 is a conceptual diagram for explaining the concept of how to perform authentication using the common encryption key.

[0115]

15 As shown in Fig. 9, the multifunction machine 10 holds a common encryption key the same as that of the server 20 within the ROM at its shipping, and the server 20 of the machine development vendor holds the data (compl.aut in an example of the plug-in) obtained by encrypting authentication information using the common encryption key together with  
20 the software components (compl.gw).

[0116]

As shown in Fig. 8, when acquiring the authentication information (step S801), the multifunction machine 10 decrypts the data with the common encryption key held within the ROM (step S802), and checks the  
25 magic number included in the decrypted data (step S803).

[0117]

When this magic number is not correct (step S804, No), the multifunction machine 10 determines that the authentication has failed, and specifies minimum resources such as only the display section and  
5 operation panel section (step S809).

[0118]

On the other hand, when the magic number is correct (step S804, Yes), the multifunction machine 10 calculates a hash value from the downloaded software component (step S805), and checks whether this  
10 hash value matches the value included in the authentication information (step S806). When these two do not match (step S806, No), the multifunction machine 10 determines that the authentication has failed, and specifies the minimum resources (step S809).

[0119]

15 When these two match (step S806, Yes), the multifunction machine 10 checks whether the right information is described in the correct format (step S807). When it is described in the correct format (step S807, Yes), the multifunction machine 10 determines that the authentication has succeeded, and specifies the resources available for  
20 the software component (step S808). When it is not described in the correct format (step S807, No), the multifunction machine 10 determines that the authentication has failed, and specifies the minimum resources (step S809).

[0120]

25 In this case, a third vendor has two methods as shown in Figs.

10A and 10B to provide a software component. More specifically, as shown in Fig. 10A, one of the methods is that the third vendor pays a registration fee to the machine development vendor and, in exchange for this, the server 20 of the machine development vendor discloses the  
5 software component to the third vendor.

[0121]

As shown in Fig. 10B, the third vendor pays an authorization fee to the machine development vendor, and the machine development vendor creates encrypted authentication information in exchange for the  
10 authorization fee to transmit the information to the server 40 of the third vendor. Such an authorization fee is changed from time to time according to setting of rights.

[0122]

(2) Performance of authentication processing with the public key

15 Fig. 11 is a conceptual diagram for explaining the concept of how to perform authentication using a public key. As shown in Fig. 11, the multifunction machine 10 holds a public key of the machine development vendor within the ROM at its shipping, and the server 20 of the machine development vendor holds the data obtained by encrypting authentication  
20 information using the secret key with respect to the public key together with the software components.

[0123]

The multifunction machine 10 acquiring the authentication information decrypts the data with the public key held within the ROM.  
25 The sequence of authentication thereafter is the same as the case where



the common key is used.

[0124]

In order for the third vendor to provide a software component, there is a method of holding the public key of the third vendor as shown in Fig. 11 and using rights of resources within the ROM at the shipping  
5 other than the two methods explained in the case of using the common key. In such a case, a larger amount of contract fee is generally paid.

[0125]

When the common key is used, the third vendor has to disclose  
10 the common key to the machine development vendor. Therefore, such a method is not realistic. But concealment of encryption is not lowered even if the public key is disclosed, therefore, any particular problem may not occur.

[0126]

15 As explained above, when the public key of the third vendor is previously held in the ROM, the third vendor can freely set the using rights of resources. However, by purchasing the encrypted setting information from the machine development vendor and decrypting the information in the multifunction machine 10 that has downloaded the information, it is  
20 possible to prevent the third vendor from its freely setting rights.

[0127]

(3) Performance of authentication processing with the certificate

Fig. 12 is a conceptual diagram for explaining the concept of how to perform authentication with a certificate. In the figure, the  
25 multifunction machine 10 holds a public key of the machine development

vendor as a certificate authority at the shipping, and the server 20 that discloses a software component holds the certificate of the public key of the server issued by the machine development vendor (certificate authority). This certificate is encrypted by the secret key of the machine development vendor (certificate authority), and the server 20 attaches this encrypted certificate to the header of the authentication information.

[0128]

The multifunction machine 10 having acquired the authentication information decrypts first the certificate attached to the authentication information by the public key of the machine development vendor (certificate authority) held within the ROM, extracts the public key of the server from this certificate when the decryption has succeeded, and decrypts the authentication information using this key. The sequence of the authentication from then on is the same as explained above.

15 [0129]

In this case, in order for the third vendor to provide a software component, as shown in Fig. 13, the third vendor pays an authorization fee to the machine development vendor and receives the certificate of the encrypted server's public key from the machine development vendor (certificate authority).

[0130]

When the method based on the public key is used, it is difficult to newly add a server of a third vendor whose public key is not recorded in the ROM at the shipping. But it is possible to add any third vendor to the machine by the method based on the certificate.

[0131]

Transmission of machine information from the multifunction machine 10 shown in Fig. 1 to the server 20 will be explained below. The multifunction machine 10 transmits the machine information such as  
5 optional hardware configuration of the multifunction machine 10, configuration of the installed software, and its serial number is transmitted as header of HTTP.

[0132]

For example, when the multifunction machine 10 is provided with  
10 the ADF as option, the header such as

X-Ricoh-MFP-Option: ADF

is added to the request of the HTTP, and as the serial number, the header such as

X-Ricoh-MFP-Serial: 123-456-789

15 is added to the request of the HTTP and notified to the server 20.

[0133]

In order to prevent the machine information from being unnecessarily leaked during this operation, (1) the header information can be encrypted, or (2) the independent authentication protocol can be  
20 used. (1) Encryption of the header information can be performed by using the common encryption key or the public key as explained with reference to the authentication. More specifically, the value of the header is encrypted by the encryption key held in the ROM of the multifunction machine 10. In the method of using the certificate, the  
25 encryption key cannot previously be acquired, therefore, this method (1)

cannot be used. Further, the server of a third vendor cannot decrypt the header information. Therefore, a server is limited to the server of the machine development vendor.

[0134]

5           When (2) the independent authentication protocol is used, the method of using the certificate can be applied. However, as explained above, authentication of the server is not performed concurrently when the software component is downloaded, but it is necessary to make a download of a software component independent from a download of the authentication protocol.

[0135]

More specifically, assuming that an initial access is made to a server, when a particular path, for example, <http://www.ricoh.co.jp/certificate> is requested and the authorized certificate is sent back in response to the request, it is determined that the server authentication has succeeded, and the request including the header encrypted by the public key included in the certificate is transmitted again. In accordance with this method, the header information is transmitted only to the authorized server, thus it is possible to further enhance the level of security. Further, the server of the third vendor can use the machine information.

[0136]

Customization of a list in the server 20 as shown in Fig. 3 will be explained below. Fig. 14 shows a diagram for explaining the case where a list is customized according to the hardware configuration of the

multifunction machine 10.

[0137]

As shown in the figure, when the multifunction machine 10 transmits a request for a list and configuration information (A, B, C, and D) to the server 20, the server 20 acquires the configuration information for the machine from the HTTP request. The server 20 then retrieves available software components based on the configuration of this machine from the software component storage section 24, and creates a list described in HTML to send the list back to the multifunction machine 10.

[0138]

Fig. 15 shows a diagram for explaining the case where the list is customized according to the machine ID of the multifunction machine 10. In this case, the multifunction machine 10 transmits the serial number (machine ID) of the machine, and the server 20 retrieves the customer database using this machine ID to acquire configuration information of the multifunction machine 10.

[0139]

The server 20 retrieves available software components from the software component storage section 24 in the same manner as that of the case shown in Fig. 14, and creates a list described in HTML to send the list back to the multifunction machine 10.

[0140]

During this operation, the components to be displayed on the list of the software components can be changed according to the contract

form of each customer. For example, the components are ranked according to the degree of complexity or usefulness, and the components displayed on the list can be changed according to the ranks of a contract fee.

5 [0141]

Although the third vendor cannot retrieve customer information through the serial number, the machine development vendor can provide only information for machine configuration to the third vendor by receiving a contract fee from the third vendor.

10 [0142]

Customization of software components in the server 20 shown in Fig. 3 will be explained below. Fig. 16 shows a diagram for explaining the case where the software components are customized in the server 20 shown in Fig. 3.

15 [0143]

As shown in Fig. 16, the server 20 confirms whether applications that operate can be created based on the creation information within the database of configuration information for applications and on the configuration information received from the multifunction machine 10, and  
20 transmits the list of the software components for the created applications to the multifunction machine 10.

[0144]

As explained above, it is possible to simply retrieve components suitable for configuration of a machine to send the list of the components  
25 and to dynamically create such a list. This case requires the server 20

to have a compile environment of the software components. But as shown in Fig. 16, the list can be dynamically created by reconfiguring software components with compile switches for each machine configuration. Accordingly, components can be provided for many machines without preparation of the components for a wide range of machine configurations.

[0145]

As explained above, in this embodiment, the multifunction machine 10 selects a desired software component from the list of the software components accumulated in the server 20, acquires the selected software component and authentication information from the server, and controls the processing operation of the software components based on the acquired authentication information. Therefore, the execution operation of the software component acquired based on the user's intention can be changed according to the result of authentication.

[0146]

Although the case where the present invention is applied to the multifunction machine has been explained in this embodiment, this invention is not limited to this case, but can be applied to any other image formation apparatuses.

[0147]

[Effects due to the Invention]

According to the invention of claim 1, the image formation apparatus selects a desired software component from a list of software components accumulated in the server displayed on the display section,

acquires the selected software component and authentication information from the server, and controls the processing operation of the software component based on the acquired authentication information. Thus, there is an advantageous effect that it is possible to obtain the image formation system capable of changing the execution operation of the software component acquired based on the user's intention according to the result of authentication.

[0148]

According to the invention of claim 2, a range of resources available for the software components, of the resources provided in the image formation apparatus, is restricted based on the authentication information. Therefore, it is possible to restrict the operation of the software component acquired from a server whose authentication has failed. Thus, there is an advantageous effect that it is possible to obtain the image formation system in which the user can avoid execution of malicious software and the machine development vendor can obtain value in exchange for authentication given to the third vendor.

[0149]

According to the invention of claim 3, when the authentication based on the authentication information has failed, it is so controlled that the display section and the operation panel section of the resources become available for the software component and all the resources become available for the software component when the authentication based on the authentication information has succeeded. Therefore, when the authentication has failed, the resources except the minimum



required resources can be prevented from being used. Thus, there is an advantageous effect that it is possible to obtain the image formation system capable of avoiding such a situation that the user wastes a large amount of paper by using the printing function or the like because of  
5 malicious software.

[0150]

According to the invention of claim 4, the authentication information includes information related to using rights of the respective resources by the software components, and it is decided whether the  
10 software components can use the resources based on the information related to the using rights. Thus, there is an advantageous effect that it is possible to obtain the image formation system capable of deciding quickly and efficiently whether the resources can be used.

[0151]

15 According to the invention of claim 5, the image formation apparatus transmits configuration information for its own apparatus to the server when the authentication based on the authentication information has succeeded. The server dynamically organizes software components executable on the image formation apparatus based on the configuration  
20 information received from the image formation apparatus, and sends the organized software components back to the image formation apparatus. Thus, there is an advantageous effect that it is possible to obtain the image formation system capable of acquiring the optimal software components that are adequate for the software configuration or the  
25 hardware configuration of the image formation apparatus when the

authentication has succeeded.

[0152]

According to the invention of claim 6, the image formation apparatus transmits its own identification information to the server. The  
5 server identifies configuration information and/or a contract form of the image formation apparatus based on the identification information received from the image formation apparatus, dynamically organizes software components executable on the image formation apparatus based on the identified configuration information and/or contract form,  
10 and sends the organized software components back to the image formation apparatus. Thus, there is an advantageous effect that it is possible to obtain the image formation system capable of acquiring the optimal software components that are adequate for the software configuration, hardware configuration, or the contract form of the image  
15 formation apparatus.

[0153]

According to the invention of claim 7, the server is a WWW server functioning on the Internet, and the image formation apparatus provides a browser with which pages described in HTML are browsed. Thus, there  
20 is an advantageous effect that it is possible to obtain the image formation system in which the image formation apparatus and the server can communicate according to the HTTP protocol and the cost of server development can be largely reduced by using the open standard such as WWW.

25 [0154]

According to the invention of claim 8, the acquired software component operates as a plug-in for the browser. Thus, there is an advantageous effect that it is possible to obtain the image formation system capable of executing easily and quickly the software component.

5 [0155]

According to the invention of claim 9, the image formation apparatus establishes a virtual machine such as Java Applet that can execute CPU-independent intermediate code, and the virtual machine executes the software components accumulated in the server in the form  
10 of the intermediate code. Thus, there is an advantageous effect that it is possible to obtain the image formation system capable of executing the same software component in various types of image formation apparatuses and of developing a software component while the component is simulated on a PC in the developing stage.

15 [0156]

According to the invention of claim 10, when a third vendor registers a software component to the server, the third vendor pays a registration fee to a vendor that manages the server. Thus, there is an advantageous effect that it is possible to obtain the image formation  
20 system capable of registering the software component by the third vendor without bringing a disadvantage to the original vendor.

[0157]

According to the invention of claim 11, the server charges the vendor for an advertisement fee of a software component each time the  
25 image formation apparatus acquires the software component from the

server. Thus, there is an advantageous effect that it is possible to obtain the image formation system capable of guaranteeing fair treatment to both the vendor that has developed the software component and the original vendor.

5 [0158]

According to the invention of claim 12, when a server of a third vendor is registered to the image formation apparatus as a server allowed to be authenticated, the third vendor pays a registration fee. Thus, there is an advantageous effect that it is possible to obtain the image formation  
10 system capable of allocating an appropriate load to the third vendor.

[0159]

According to the invention of claim 13, a using charge of the image formation apparatus and/or a registration fee paid by a third vendor is changed according to a range of the resources available for the image  
15 formation apparatus. Thus, there is an advantageous effect that it is possible to obtain the image formation system capable of collecting an appropriate using charge and/or registration fee according to the available range of the resources.

[0160]

20 According to the invention of claim 14, the image formation apparatus selects a desired software component from a list of software components accumulated in a server displayed on a display section, acquires the selected software component and authentication information from the server, and controls the processing operation of the software  
25 component based on the acquired authentication information. Thus,

there is an advantageous effect that it is possible to obtain the software acquisition method capable of changing the execution operation of the software component acquired based on the user's intention according to the result of authentication.

5 [0161]

According to the invention of claim 15, the range of resources available for software components, of the resources provided in the image formation apparatus, is restricted based on the authentication information. Therefore, it is possible to restrict the operation of the software component from a server whose authentication has failed. Thus, there is an advantageous effect that it is possible to obtain the software acquisition method in which the user can avoid execution of malicious software and the machine development vendor can obtain value in exchange for authentication given to the third vendor.

15 [0162]

According to the invention of claim 16, when authentication based on the authentication information has failed, it is so controlled that the display section and the operation panel section of the resources become available for the software components and all the resources become available for the software components when the authentication based on the authentication information has succeeded. Therefore, when the authentication has failed, the resources except the minimum required resources can be prevented from being used. Thus, there is an advantageous effect that it is possible to obtain the software acquisition method capable of avoiding such a situation that the user wastes a large

amount of paper by using the printing function or the like because of malicious software.

[0163]

According to the invention of claim 17, the authentication  
5 information includes information related to using rights of the respective  
resources by the software components, and it is decided whether the  
software components can use the resources based on the information  
related to the using rights. Thus, there is an advantageous effect that it  
is possible to obtain the software acquisition method capable of deciding  
10 quickly and efficiently whether the resources can be used.

[0164]

According to the invention of claim 18, the image formation  
apparatus transmits configuration information for its own apparatus to the  
server when the authentication based on the authentication information  
15 has succeeded. The server dynamically organizes software components  
executable on the image formation apparatus based on the configuration  
information received from the image formation apparatus, and sends the  
organized software components back to the image formation apparatus.  
Thus, there is an advantageous effect that it is possible to obtain the  
20 software acquisition method capable of acquiring the optimal software  
components that are adequate for the software configuration or the  
hardware configuration of the image formation apparatus when the  
authentication has succeeded.

[0165]

25 According to the invention of claim 19, the image formation

apparatus transmits its own identification information to the server. The server identifies configuration information and/or a contract form of the image formation apparatus based on the identification information received from the image formation apparatus, dynamically organizes  
5 software components executable on the image formation apparatus based on the identified configuration information and/or contract form, and sends the organized software components back to the image formation apparatus. Thus, there is an advantageous effect that it is possible to obtain the software acquisition method capable of acquiring  
10 the optimal software components that are adequate for the software configuration, hardware configuration, or the contract form of the image formation apparatus.

[0166]

According to the invention of claim 20, the server is a WWW  
15 server functioning on the Internet, and the image formation apparatus provides a browser with which pages described in HTML are browsed. Thus, there is an advantageous effect that it is possible to obtain the software acquisition method in which the image formation apparatus and the server can communicate according to the HTTP protocol and the cost  
20 of server development can be largely reduced by using the open standard such as WWW.

[0167]

According to the invention of claim 21, the acquired software component operates as a plug-in for the browser. Thus, there is an  
25 advantageous effect that it is possible to obtain the software acquisition

method capable of executing easily and quickly the software component.

[0168]

According to the invention of claim 22, the image formation apparatus establishes a virtual machine such as Java Applet that can  
5 execute CPU-independent intermediate code, and the virtual machine executes the software components accumulated in the server in the form of the intermediate code. Thus, there is an advantageous effect that it is possible to obtain the software acquisition method capable of executing the same software component in various types of image formation  
10 apparatuses and of developing a software component while the component is simulated on a PC in the developing stage.

[0169]

According to the invention of claim 23, when a third vendor registers a software component to the server, the third vendor pays a  
15 registration fee to a vendor that manages the server. Thus, there is an advantageous effect that it is possible to obtain the software acquisition method capable of registering the software component by the third vendor without bringing a disadvantage to the original vendor.

[0170]

20 According to the invention of claim 24, the server charges the vendor for an advertisement fee of a software component each time the image formation apparatus acquires the software component from the server. Thus, there is an advantageous effect that it is possible to obtain the software acquisition method capable of guaranteeing fair treatment to  
25 both the vendor that has developed the software component and the



original vendor.

[0171]

According to the invention of claim 25, when a server of a third vendor is registered to the image formation apparatus as a server allowed  
5 to be authenticated, the third vendor pays a registration fee. Thus, there is an advantageous effect that it is possible to obtain the software acquisition method capable of allocating an appropriate load to the third vendor.

[0172]

10 According to the invention of claim 26, a using charge of the image formation apparatus and/or a registration fee paid by a third vendor is changed according to a range of the resources available for the image formation apparatus. Thus, there is an advantageous effect that it is possible to obtain the software acquisition method capable of collecting  
15 an appropriate using charge and/or registration fee according to the available range of the resources.

[0173]

According to the invention of claim 27, by recording the program for making a computer execute one of the methods according to any one  
20 of claims 14 to 26 in the recording medium, the program becomes machine readable. Accordingly, there is an advantageous effect that it is possible to obtain the recording medium capable of performing one of the operations according to any one of claims 14 to 26 by the computer.

[0174]

25 The present document incorporates by reference the entire

contents of Japanese priority documents, 2001-094342 filed in Japan on March 28, 2001.

[Brief Description of the Drawings]

5 [Fig. 1]

Fig. 1 is a block diagram showing a system construction of the image formation system and a hardware configuration of the multifunction machine according to an embodiment of this invention.

[Fig. 2]

10 Fig. 2 is a block diagram showing a software configuration of the multifunction machine shown in Fig. 1.

[Fig. 3]

Fig. 3 is a functional block diagram showing a configuration of the server shown in Fig. 1.

15 [Fig. 4]

Fig. 4 is a flowchart showing a processing sequence when downloading is executed by a plug-in.

[Fig. 5]

20 Fig. 5(a) shows URLs of software components owned by the server, and Fig. 5(b) shows an example of HTML description.

[Fig. 6]

Fig. 6 is a flow chart showing a processing sequence when the software component is downloaded using Java.

[Fig. 7]

25 Fig. 7(a) shows an example of an HTML file as a target to be

linked, and Fig. 7(b) shows a software configuration of the multifunction machine in the above case.

[Fig. 8]

Fig. 8 is a flowchart showing a processing sequence of the multifunction machine when authentication is performed using a common encryption key.

[Fig. 9]

Fig. 9 is a conceptual diagram for explaining a concept of how to perform authentication using the common encryption key.

10 [Fig. 10]

Fig. 10(a) and (b) show diagrams for explaining how a third vendor provides a software component.

[Fig. 11]

Fig. 11 is a conceptual diagram for explaining a concept of how to perform authentication using a public key.

[Fig. 12]

Fig. 12 is a conceptual diagram for explaining a concept of how to perform authentication using a certificate.

[Fig. 13]

20 Fig. 13 is a diagram for explaining how a third vendor provides a software component.

[Fig. 14]

Fig. 14 is a diagram for explaining a case where a list is customized according to the hardware configuration of the multifunction machine.

[Fig. 15]

Fig. 15 is a diagram for explaining a case where a list is customized according to the machine ID of the multifunction machine.

[Fig. 16]

5 Fig. 16 is a diagram for explaining how the software components are customized in the server shown in Fig. 3.

[Description of Signs]

	10	Multifunction machine
10	11	CPU
	12	ROM
	13	R A M
	14	Flash memory
	15	FAX controller
15	16	Scanner
	17	Plotter
	18	Llarge-capacity storage device
	19	Network I/F section
	20, 40	Server
20	21	Interface section
	22	Encryption processing section
	23	Authentication information transmission section
	24	Software component storage section
	25	Customization processing section
25	26	Control section

	30	Network
	101	B&W LP
	102	Color LP
	103	Other hardware resources
5	110	Software group
	120	Pplatform
	130	Application
	131	Printer application
	132	Copier application
10	133	Fax application
	134	Scanner application
	135	WWW Browser
	136	Downloading application
	137	Authentication processing application
15	141	ECS
	142	MCS
	143	OCS
	144	FCS
	145	NCS

[Type of Document] Abstract

[Abstract]

[Object] To legitimately and efficiently acquire software adequate for an image formation apparatus after the image formation apparatus is

5 activated and execute the software.

[Means] A multifunction machine 10 selects a desired software component from a list of software components accumulated in a server 20, acquires the selected software component and authentication information from the server, and controls the processing operation of the  
10 software component based on the acquired authentication information.

[Selected Figure] Fig. 4

FIG.1

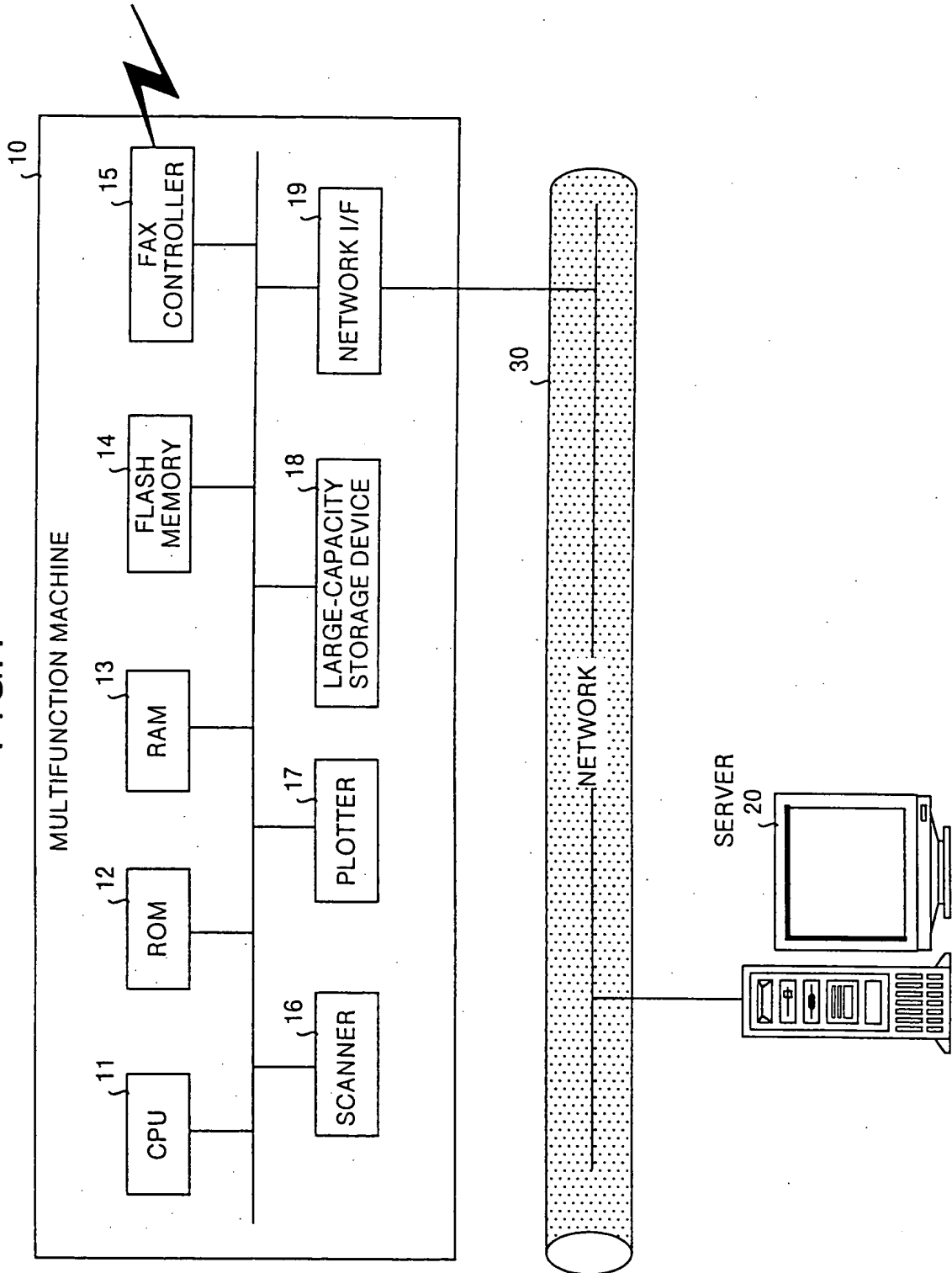


FIG.2 MULTIFUNCTION MACHINE

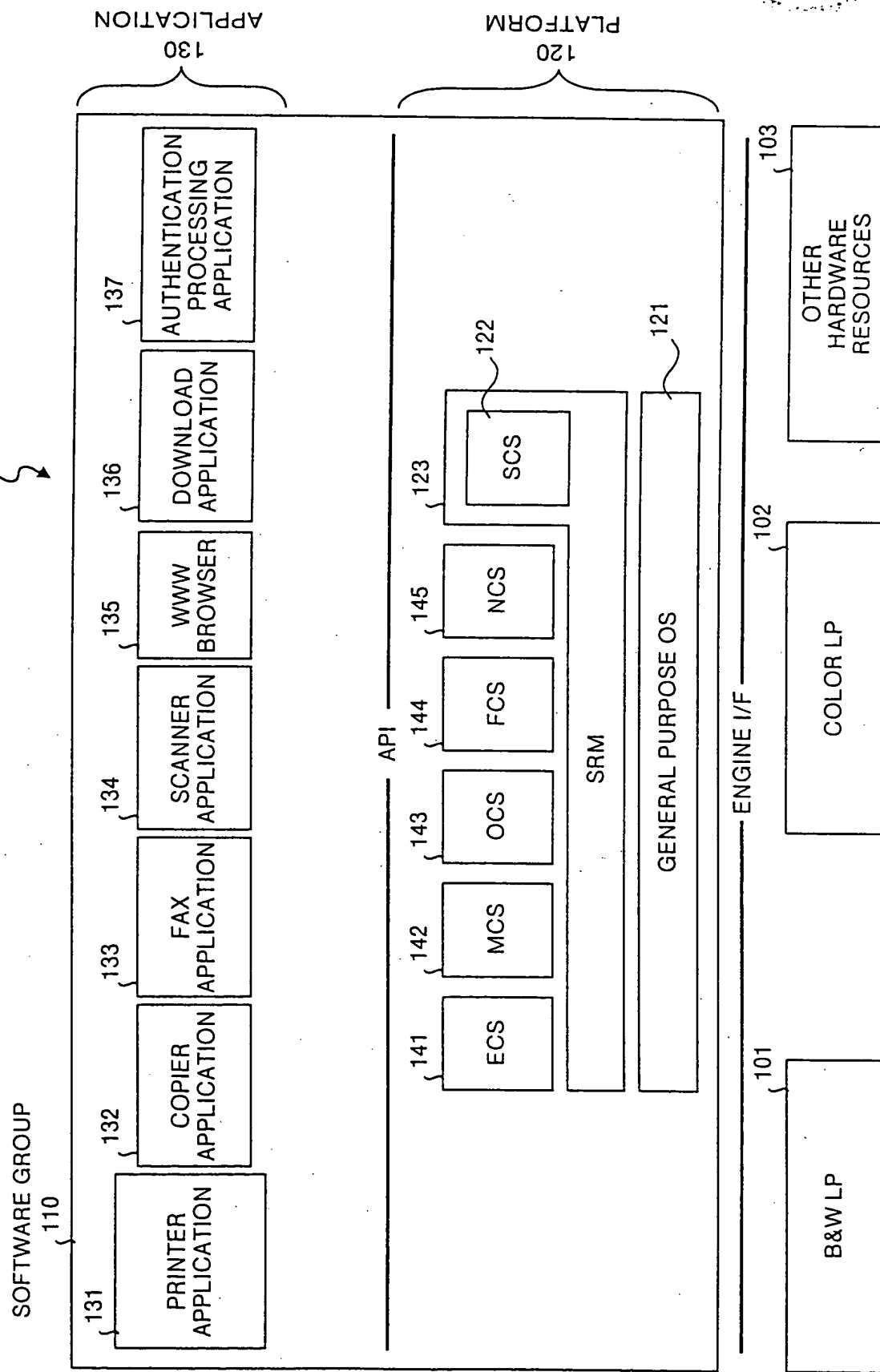




FIG.3

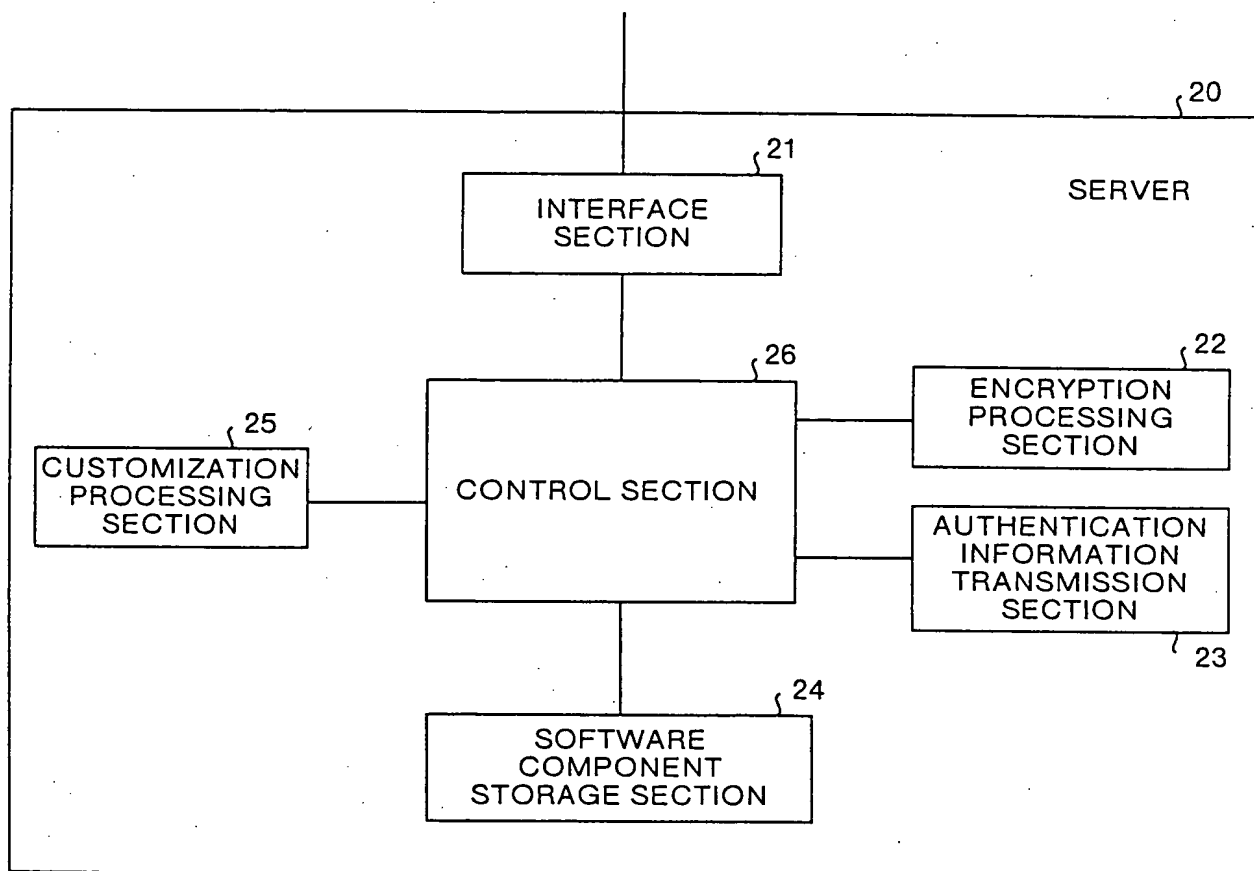
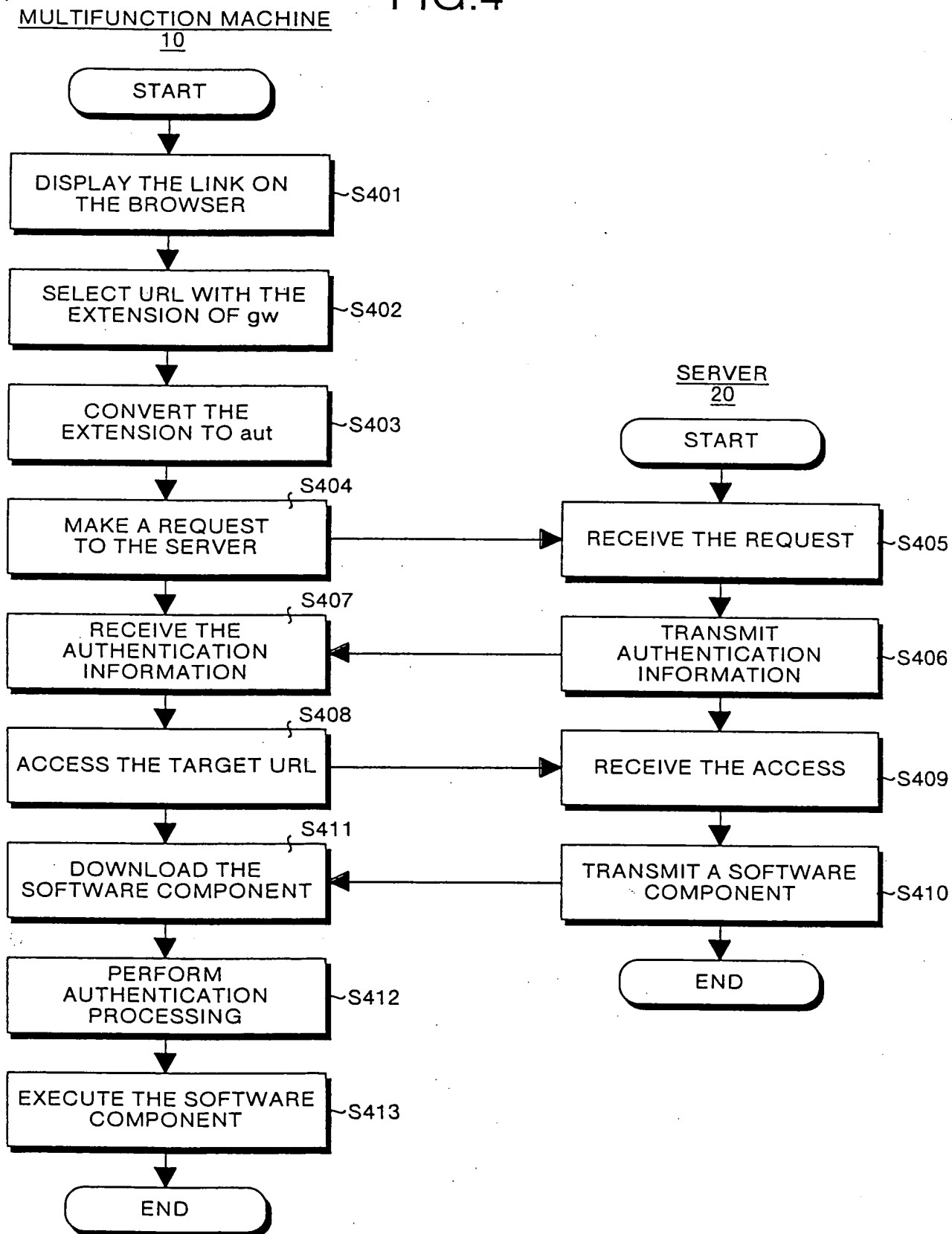
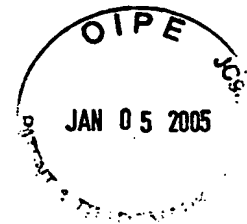


FIG.4





## FIG.5

(a)

[http://www.ricoh.co.jp/component/comp\\_list.html](http://www.ricoh.co.jp/component/comp_list.html)

HTML FILE INCLUDING THE LINK TO THE LIST OF COMPONENTS

[http://www.ricoh.co.jp/component/comp\\_1.gw](http://www.ricoh.co.jp/component/comp_1.gw)

SOFTWARE COMPONENT 1

[http://www.ricoh.co.jp/component/comp\\_1.aut](http://www.ricoh.co.jp/component/comp_1.aut)

AUTHENTICATION INFORMATION FOR THE SOFTWARE COMPONENT 1

<http://www.ricoh.co.jp/component/comp2.gw>

SOFTWARE COMPONENT 2

<http://www.ricoh.co.jp/component/comp2.aut>

AUTHENTICATION INFORMATION FOR THE SOFTWARE COMPONENT 2

:

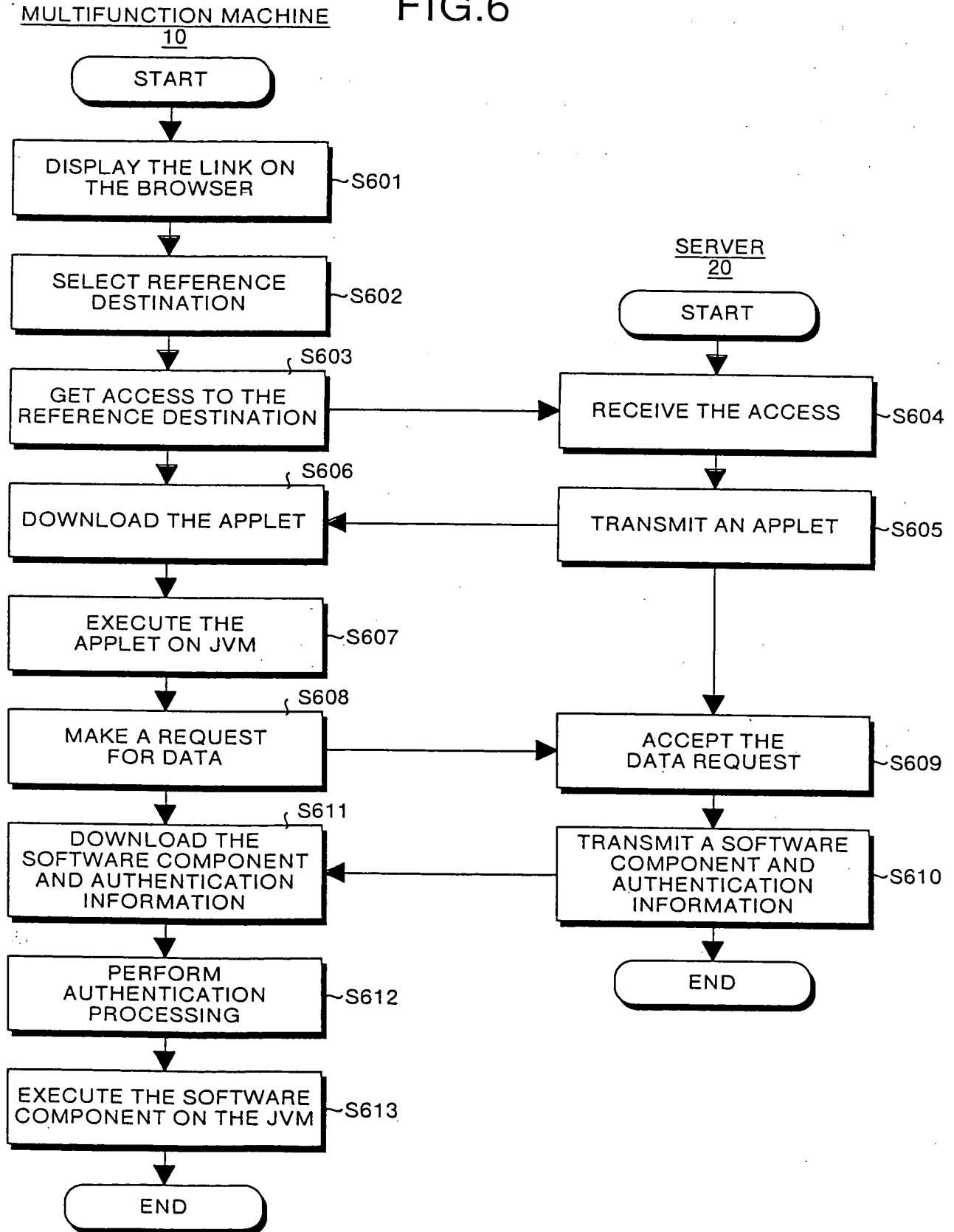
:

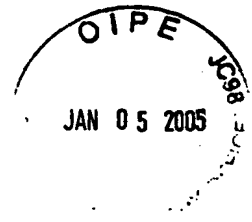
## FIG.5

(b)

```
<html>
<head>
  <title>Software Component List</title>
</head>
<body>
  <h1>Component List</h1>
  <u1>
    <li><a href="comp1.gw">COMPONENT1</a>
    <li><a href="comp2.gw">COMPONENT2</a>
  </u1>
</body>
</html>
```

FIG.6





(a)

FIG.7

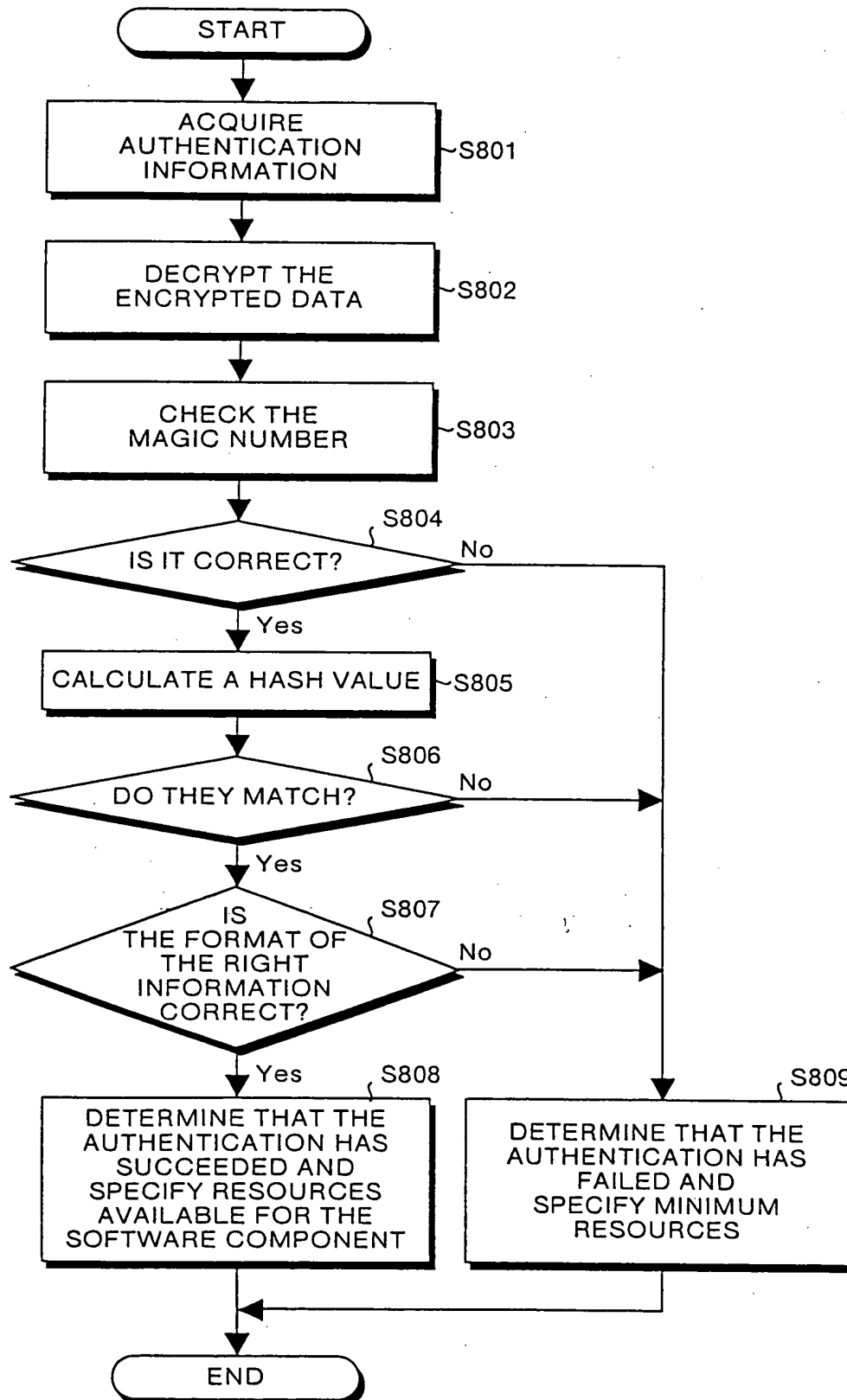
```
<html>
<head>
  <title> Component 1</title>
</head>
<body>
  <applet code="SoftwareComponentLoader.class"width="640"height="400">
    <param name="software"value="comp1.class">
    <param name="authentication"value="comp1.aut">
  </applet>
</body>
</html>
```

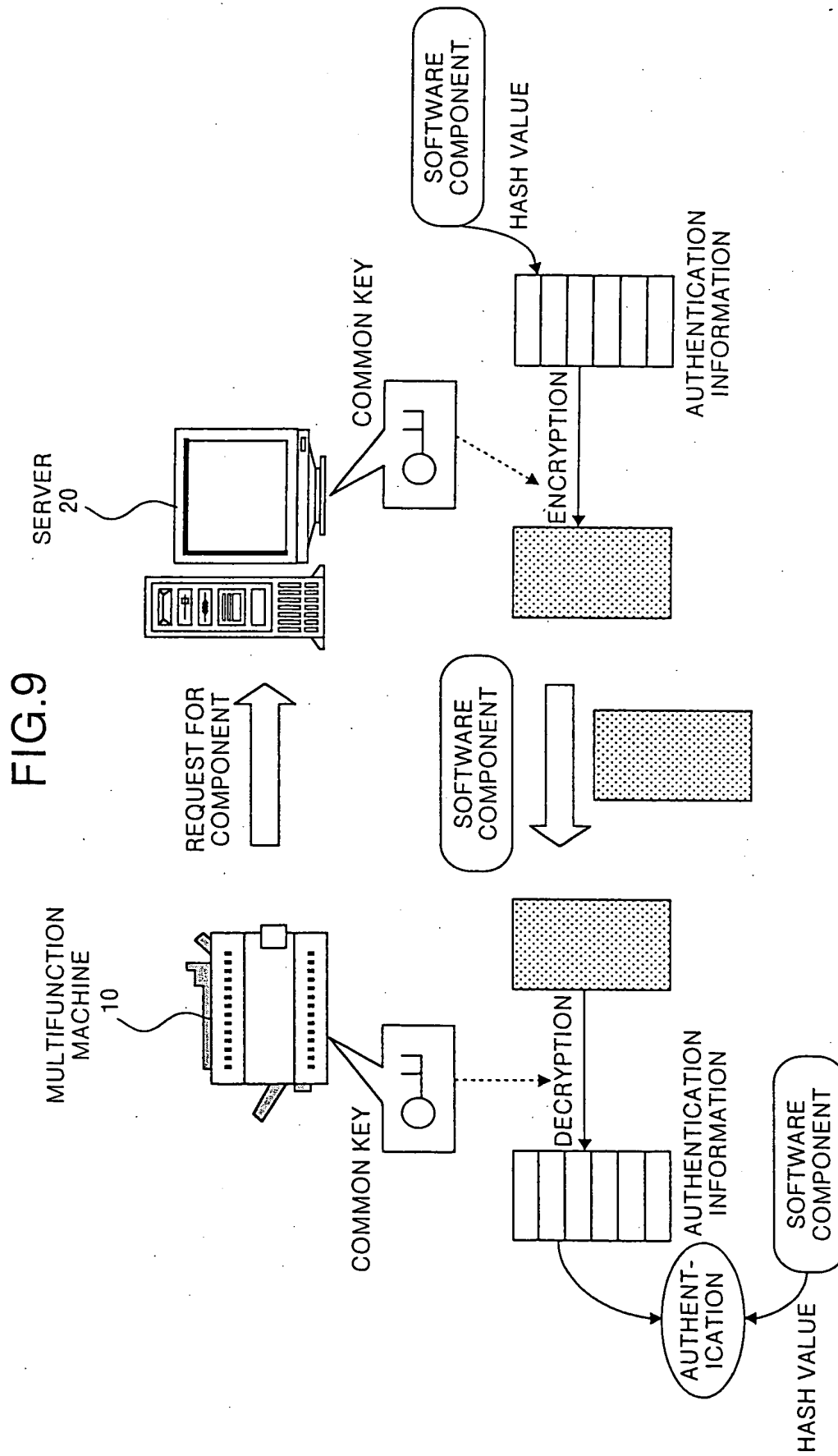
(b)

FIG.7

APPLICATION (SOFTWARE COMPONENT)					
CONTROL CLASS				STANDARD CLASS	
JVM					
API					
ECS	MCS	FCS	SCS	OCS	NCS
OS					

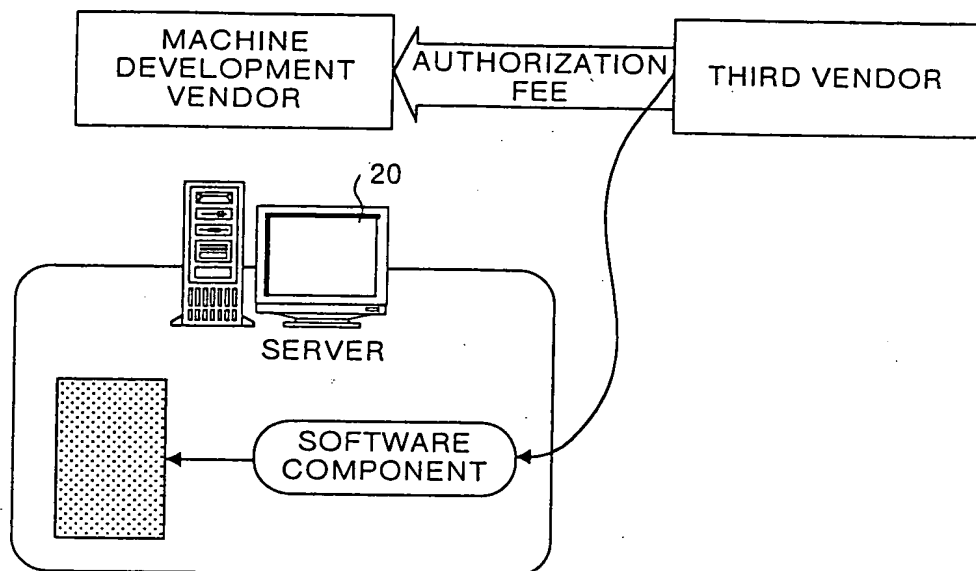
FIG.8







(a) FIG.10.



(b) FIG.10

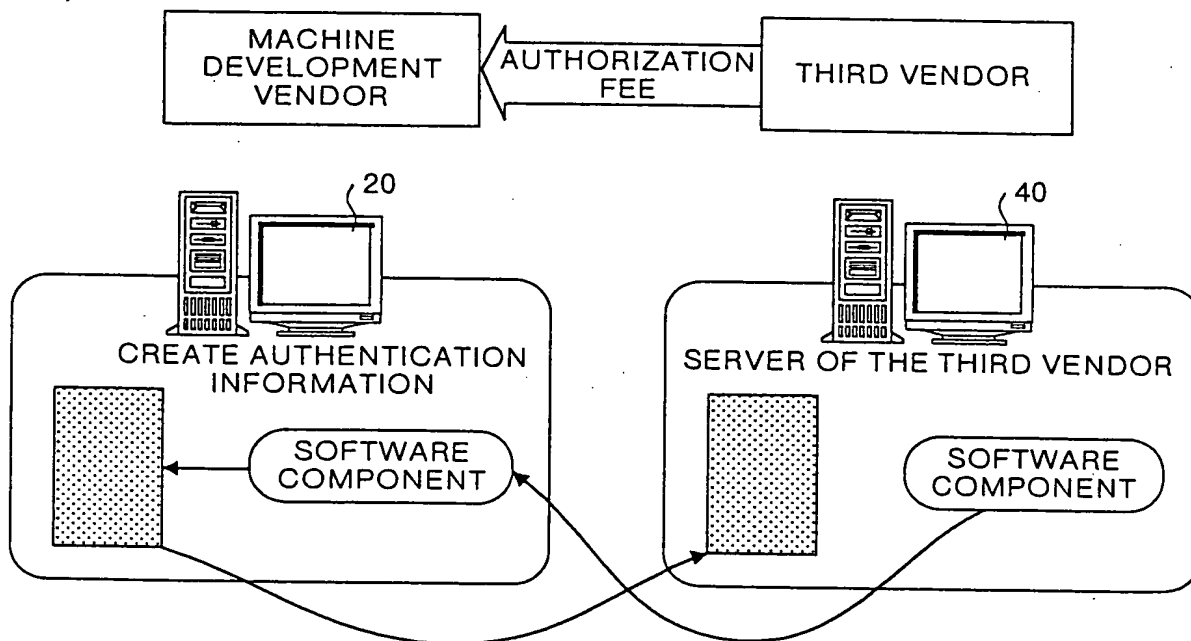






FIG.11

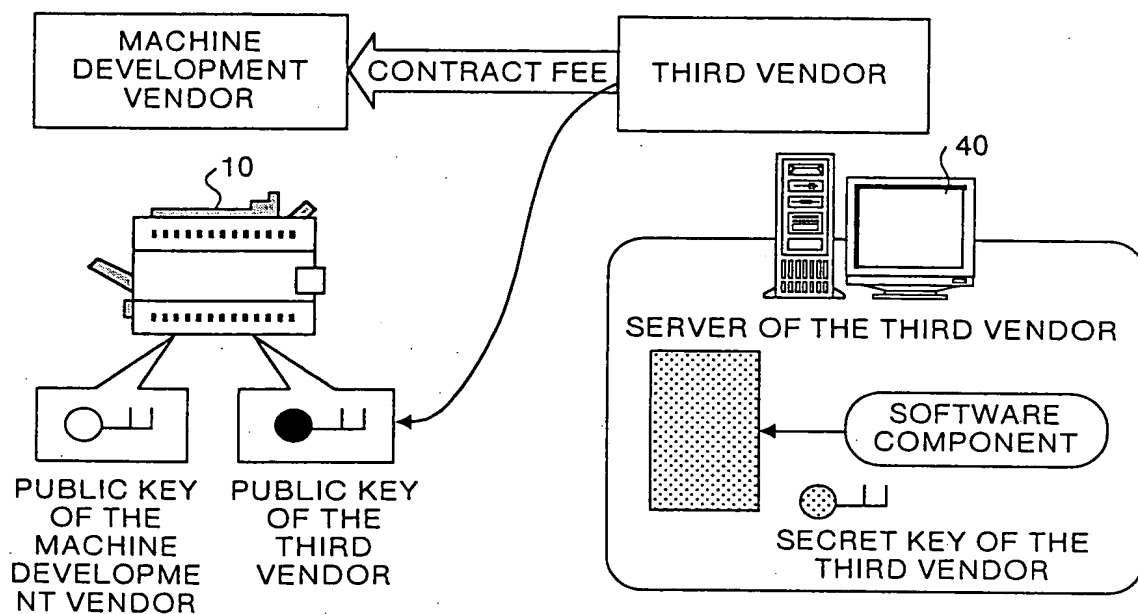


FIG.12

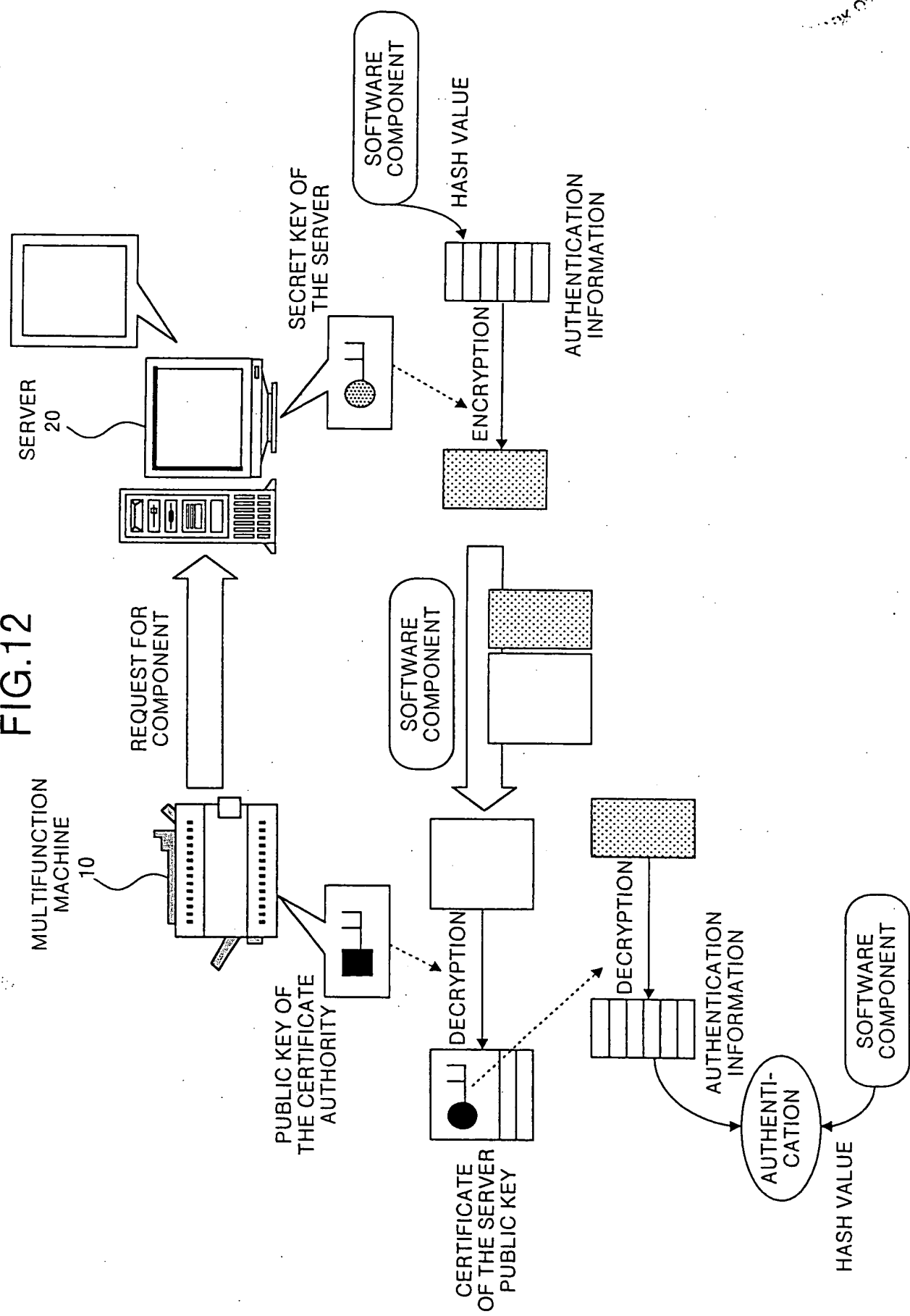


FIG.13

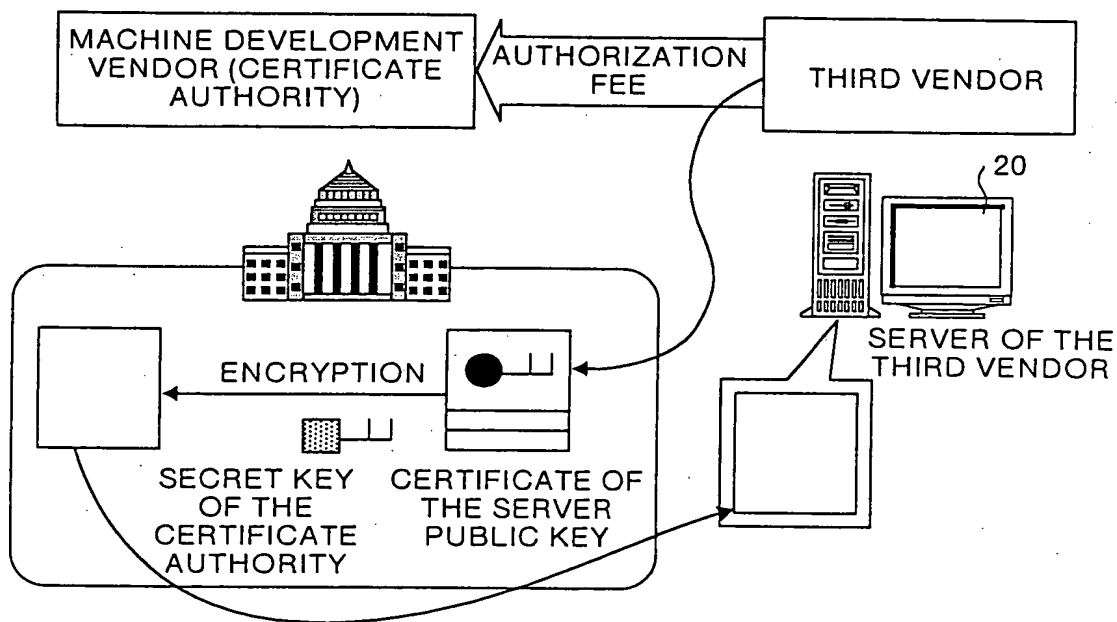


FIG.14

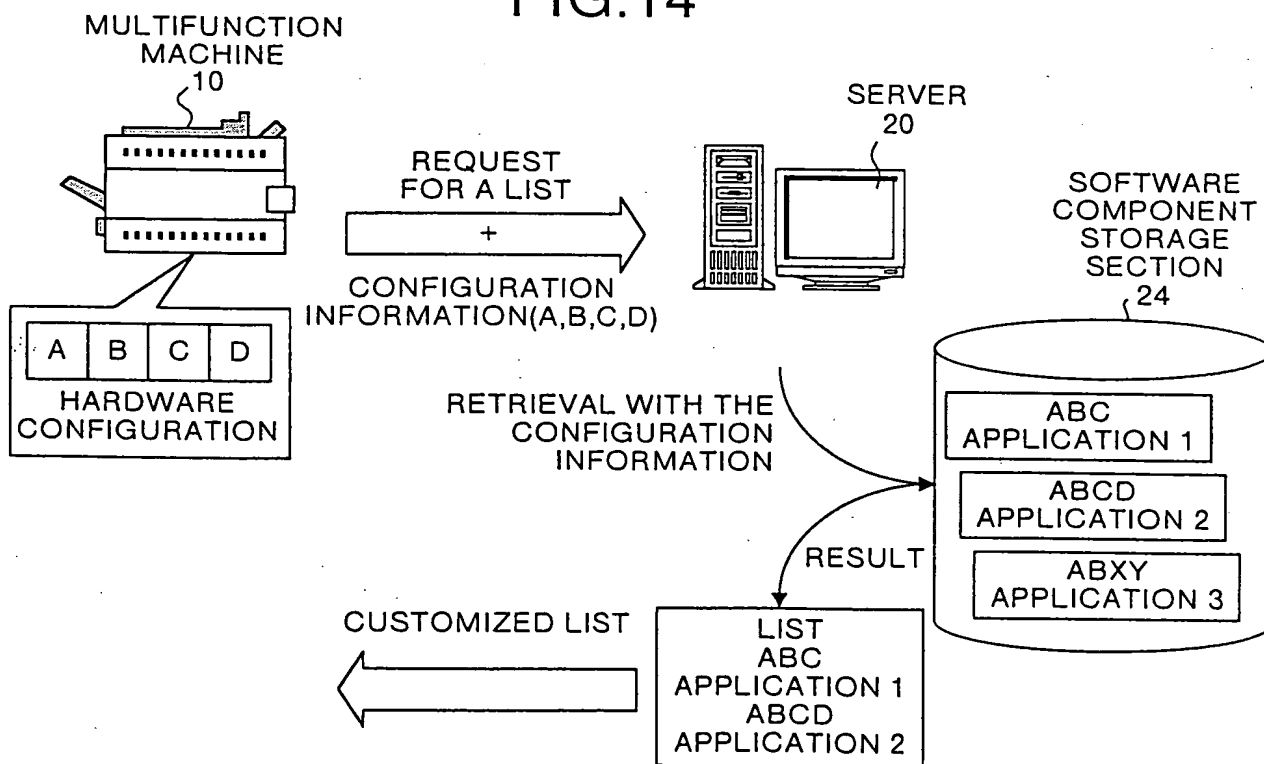
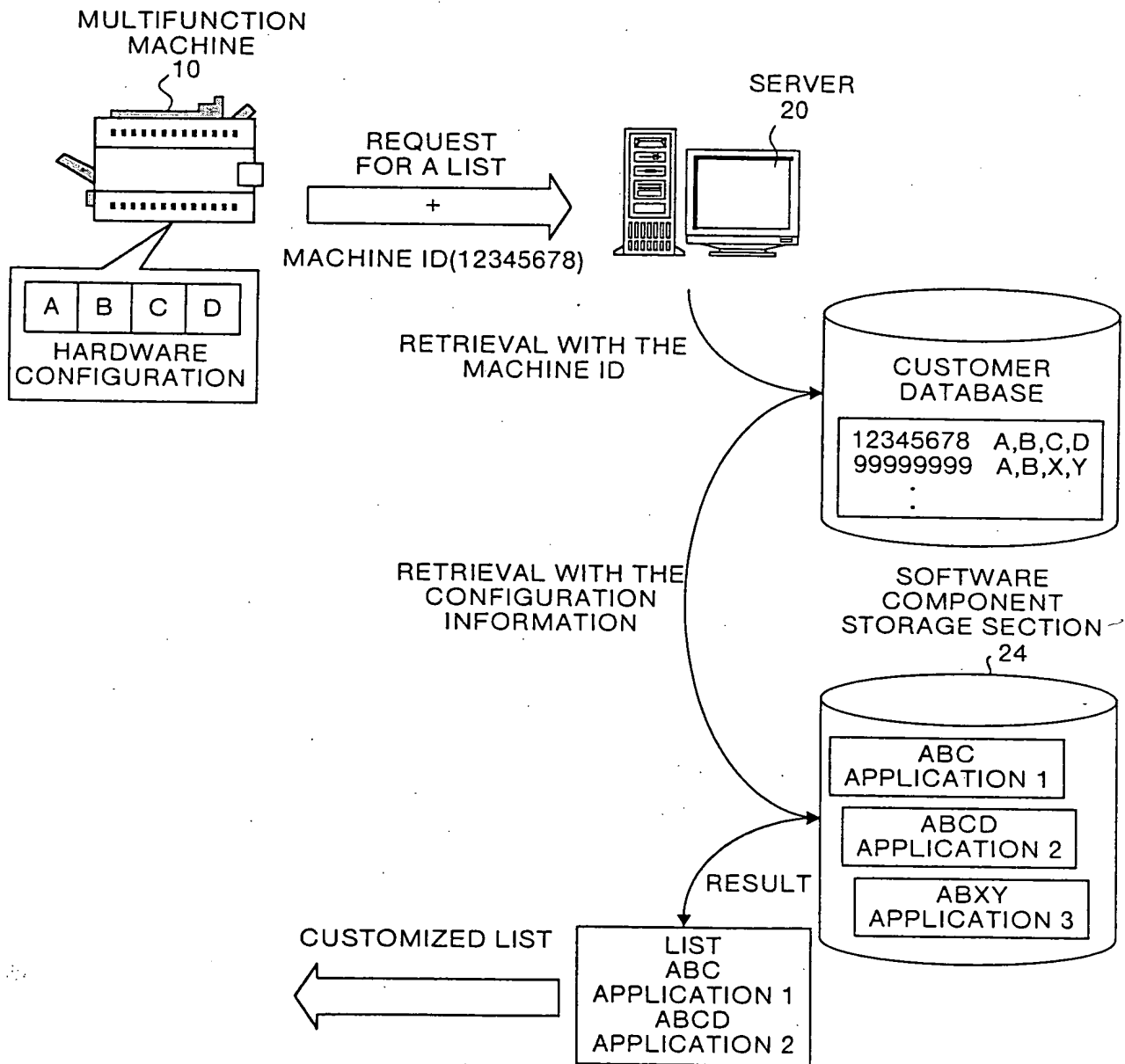




FIG.15



MULTIFUNCTION MACHINE

10

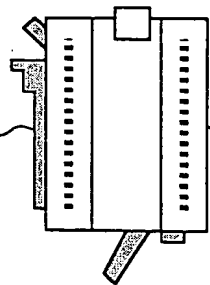
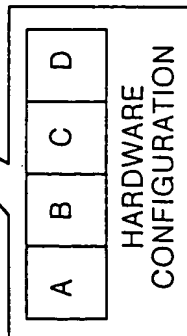


IMAGE I/O MACHINE



REQUEST  
FOR A LIST

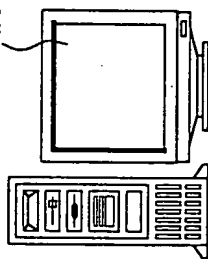
+

CONFIGURATION  
INFORMATION(A,B,C,D)

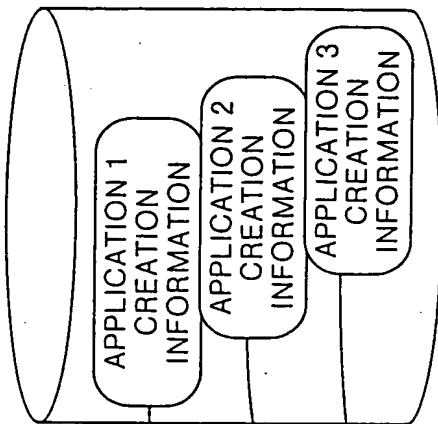
FIG.16

SERVER

20



DATABASE OF CONFIGURATION  
INFORMATION FOR  
APPLICATIONS



CONFIGURATION  
INFORMATION

COMPILER

APPLICATION 3 THAT OPERATES  
CANNOT BE CREATED WITH THIS  
CONFIGURATION INFORMATION

ABC  
APPLICATION 1

ABCD  
APPLICATION 2

LIST  
ABC  
APPLICATION 1  
ABCD  
APPLICATION 2

LIST OF THE CUSTOMIZED  
COMPONENTS

